ID: 02ab4847-0190-4760-8280-c063c2340002

of 8 Dec 2022, C-694/20 (  
Orde van Vlaamse Balies and Others  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
   
JUDGMENT OF THE COURT (Grand Chamber)  
8 December 2022 (\*)  
(Reference for a preliminary ruling – Administrative cooperation in the field of taxation – Mandatory automatic exchange of information in relation to reportable cross-border arrangements – Directive 2011/16/EU, as amended by Directive (EU) 2018/822 – Article 8ab(5) – Validity – Legal professional privilege of the lawyer – Exemption from the reporting obligation for the benefit of lawyer-intermediaries subject to legal professional privilege – Obligation on that lawyer-intermediary to notify any other intermediary who is not his or her client of that intermediary’s reporting obligations – Articles 7 and 47 of the Charter of Fundamental Rights of the European Union)  
In Case C-694/20,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Grondwettelijk Hof (Constitutional Court, Belgium), made by decision of 17 December 2020, received at the Court on 21 December 2020, in the proceedings  
Orde van Vlaamse Balies,  
IG,  
Belgian Association of Tax Lawyers,  
CD,  
JU  
v  
Vlaamse Regering,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, A. Prechal, K. Jürimäe, P.G. Xuereb, L.S. Rossi and D. Gratsias, Presidents of Chambers, F. Biltgen, N. Piçarra, I. Jarukaitis, N. Jääskinen, N. Wahl, I. Ziemele and J. Passer (Rapporteur), Judges,  
Advocate General: A. Rantos,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 25 January 2022,  
after considering the observations submitted on behalf of:  
–        Orde van Vlaamse Balies and IG, by S. Eskenazi and P. Wouters, advocaten,  
–        Belgian Association of Tax Lawyers, CD and JU, by P. Malherbe, avocat, and P. Verhaeghe, advocaat,  
–        the Belgian Government, by S. Baeyens, J.-C. Halleux and C. Pochet, acting as Agents, and by M. Delanote, advocaat,  
–        the Czech Government, by J. Očková, M. Smolek and J. Vláčil, acting as Agents,  
–        the French Government, by R. Bénard, A.-L. Desjonquères, E. de Moustier and É. Toutain, acting as Agents,  
–        the Latvian Government, by J. Davidoviča, I. Hūna and K. Pommere, acting as Agents,  
–        the Council of the European Union, by E. Chatziioakeimidou, I. Gurov and S. Van Overmeire, acting as Agents,  
–        the European Commission, by W. Roels and P. Van Nuffel, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 5 April 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the validity of Article 8ab(5) of Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (OJ 2011 L 64, p. 1), as amended by Council Directive (EU) 2018/822 of 25 May 2018 (OJ 2018 L 139, p. 1) (‘amended Directive 2011/16’), in the light of Articles 7 and 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between, on the one hand, the Orde van Vlaamse Balies (Flemish Bar Association, Belgium), the Belgian Association of Tax Lawyers, IG, CD and JU, three lawyers, and, on the other, the Vlaamse Regering (Flemish Government, Belgium) concerning the validity of certain provisions of Flemish legislation on administrative cooperation in the field of taxation.  
   
Legal context  
   
European Union law  
   
Directive 2011/16  
3        Directive 2011/16 has established a system of cooperation between the national tax authorities of the Member States and lays down the rules and procedures to be applied when exchanging information for tax purposes.  
   
Directive 2018/822  
4        Directive 2011/16 has been amended on several occasions, in particular by Directive 2018/822. That directive introduced an obligation to report any potentially aggressive tax-planning cross-border tax arrangements to the competent authorities. In that regard, recitals 2, 4, 6, 8, 9 and 18 of Directive 2018/822 state the following:  
‘(2)      Member States find it increasingly difficult to protect their national tax bases from erosion as tax-planning structures have evolved to be particularly sophisticated and often take advantage of the increased mobility of both capital and persons within the internal market. … It is therefore critical that Member States’ tax authorities obtain comprehensive and relevant information about potentially aggressive tax arrangements. Such information would enable those authorities to react promptly against harmful tax practices and to close loopholes by enacting legislation or by undertaking adequate risk assessments and carrying out tax audits. …  
…  
(4)      Recognising how a transparent framework for developing business activity could contribute to clamping down on tax avoidance and evasion in the internal market, the [European] Commission has been called on to embark on initiatives on the mandatory disclosure of information on potentially aggressive tax-planning arrangements along the lines of Action 12 of the [Organisation for Economic Co-operation and Development (OECD)] Base Erosion and Profit Shifting (BEPS) Project. In this context, the European Parliament has called for tougher measures against intermediaries who assist in arrangements that may lead to tax avoidance and evasion. It is also important to note that in the G7 Bari Declaration of 13 May 2017 on fighting tax crimes and other illicit financial flows, the OECD was asked to start discussing possible ways to address arrangements designed to circumvent reporting under the [Common Reporting Standard (CRS)] or aimed at providing beneficial owners with the shelter of non-transparent structures, considering also model mandatory disclosure rules inspired by the approach taken for avoidance arrangements outlined within the BEPS Action 12 Report.  
…  
(6)      The reporting of potentially aggressive cross-border tax-planning arrangements can contribute effectively to the efforts for creating an environment of fair taxation in the internal market. In this light, an obligation for intermediaries to inform tax authorities … would constitute a step in the right direction. …  
…  
(8)      To ensure the proper functioning of the internal market and to prevent loopholes in the proposed framework of rules, the reporting obligation should be placed upon all actors that are usually involved in designing, marketing, organising or managing the implementation of a reportable cross-border transaction or a series of such transactions, as well as those who provide assistance or advice. It should not be ignored either that, in certain cases, the reporting obligation would not be enforceable upon an intermediary due to a legal professional privilege or where there is no intermediary because, for instance, the taxpayer designs and implements a scheme in-house. It would thus be crucial that, in such circumstances, tax authorities do not lose the opportunity to receive information about tax-related arrangements that are potentially linked to aggressive tax planning. It would therefore be necessary to shift the reporting obligation to the taxpayer who benefits from the arrangement in such cases.  
(9)      Aggressive tax-planning arrangements have evolved over the years to become increasingly more complex and are always subject to constant modifications and adjustments as a reaction to defensive countermeasures by the tax authorities. Taking this into consideration, it would be more effective to endeavour to capture potentially aggressive tax-planning arrangements through the compiling of a list of the features and elements of transactions that present a strong indication of tax avoidance or abuse rather than to define the concept of aggressive tax planning. Those indications are referred to as “hallmarks”.  
…  
(18)      This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter …’  
Amended Directive 2011/16  
5        Article 3 of amended Directive 2011/16 entitled ‘Definitions’ provides:  
‘For the purposes of this Directive the following definitions shall apply:  
1.      “competent authority” of a Member State means the authority which has been designated as such by that Member State. When acting pursuant to this Directive, the central liaison office, a liaison department or a competent official shall also be deemed to be competent authorities by delegation according to Article 4;  
…  
18.      “cross-border arrangements” means an arrangement concerning either more than one Member State or a Member State and a third country where at least one of the following conditions is met:  
(a)      not all of the participants in the arrangement are resident for tax purposes in the same jurisdiction;  
(b)      one or more of the participants in the arrangement is simultaneously resident for tax purposes in more than one jurisdiction;  
(c)      one or more of the participants in the arrangement carries on a business in another jurisdiction through a permanent establishment situated in that jurisdiction and the arrangement forms part or the whole of the business of that permanent establishment;  
(d)      one or more of the participants in the arrangement carries on an activity in another jurisdiction without being resident for tax purposes or creating a permanent establishment situated in that jurisdiction;  
(e)      such arrangement has a possible impact on the automatic exchange of information or the identification of beneficial ownership.  
…  
19.      “reportable cross-border arrangement” means any cross-border arrangement that contains at least one of the hallmarks set out in Annex IV;  
20.      “hallmark” means a characteristic or feature of a cross-border arrangement that presents an indication of a potential risk of tax avoidance, as listed in Annex IV;  
21.      “intermediary” means any person that designs, markets, organises or makes available for implementation or manages the implementation of a reportable cross-border arrangement.  
It also means any person that, having regard to the relevant facts and circumstances and based on available information and the relevant expertise and understanding required to provide such services, knows or could be reasonably expected to know that they have undertaken to provide, directly or by means of other persons, aid, assistance or advice with respect to designing, marketing, organising, making available for implementation or managing the implementation of a reportable cross-border arrangement. Any person shall have the right to provide evidence that such person did not know and could not reasonably be expected to know that that person was involved in a reportable cross-border arrangement. For this purpose, that person may refer to all relevant facts and circumstances as well as available information and their relevant expertise and understanding.  
In order to be an intermediary, a person shall meet at least one of the following additional conditions:  
(a)      be resident for tax purposes in a Member State;  
(b)      have a permanent establishment in a Member State through which the services with respect to the arrangement are provided;  
(c)      be incorporated in, or governed by the laws of, a Member State;  
(d)      be registered with a professional association related to legal, taxation or consultancy services in a Member State.  
22.      “relevant taxpayer” means any person to whom a reportable cross-border arrangement is made available for implementation, or who is ready to implement a reportable cross-border arrangement or has implemented the first step of such an arrangement.  
…  
24.      “marketable arrangement” means a cross-border arrangement that is designed, marketed, ready for implementation or made available for implementation without a need to be substantially customised.  
25.      “bespoke arrangement” means any cross-border arrangement that is not a marketable arrangement.’  
6        Article 8ab of amended Directive 2011/16, entitled ‘Scope and conditions of mandatory automatic exchange of information on reportable cross-border arrangements’, was inserted by Article 1(2) of Directive 2018/822 and states:  
‘1.      Each Member State shall take the necessary measures to require intermediaries to file information that is within their knowledge, possession or control on reportable cross-border arrangements with the competent authorities within 30 days beginning:  
(a)      on the day after the reportable cross-border arrangement is made available for implementation; or  
(b)      on the day after the reportable cross-border arrangement is ready for implementation; or  
(c)      when the first step in the implementation of the reportable cross-border arrangement has been made,  
whichever occurs first.  
Notwithstanding the first subparagraph, intermediaries referred to in the second paragraph of point 21 of Article 3 shall also be required to file information within 30 days beginning on the day after they provided, directly or by means of other persons, aid, assistance or advice.  
2.      In the case of marketable arrangements, Member States shall take the necessary measures to require that a periodic report be made by the intermediary every 3 months providing an update which contains new reportable information as referred to in points (a), (d), (g) and (h) of paragraph 14 that has become available since the last report was filed.  
…  
5.      Each Member State may take the necessary measures to give intermediaries the right to a waiver from filing information on a reportable cross-border arrangement where the reporting obligation would breach the legal professional privilege under the national law of that Member State. In such circumstances, each Member State shall take the necessary measures to require intermediaries to notify, without delay, any other intermediary or, if there is no such intermediary, the relevant taxpayer of their reporting obligations under paragraph 6.  
Intermediaries may only be entitled to a waiver under the first subparagraph to the extent that they operate within the limits of the relevant national laws that define their professions.  
6.      Each Member State shall take the necessary measures to require that, where there is no intermediary or the intermediary notifies the relevant taxpayer or another intermediary of the application of a waiver under paragraph 5, the obligation to file information on a reportable cross-border arrangement lie with the other notified intermediary, or, if there is no such intermediary, with the relevant taxpayer.  
…  
9.      Each Member State shall take the necessary measures to require that, where there is more than one intermediary, the obligation to file information on the reportable cross-border arrangement lie with all intermediaries involved in the same reportable cross-border arrangement.  
An intermediary shall be exempt from filing the information only to the extent that it has proof, in accordance with national law, that the same information referred to in paragraph 14 has already been filed by another intermediary.  
…  
13.      The competent authority of a Member State where the information was filed pursuant to paragraphs 1 to 12 … shall … communicate … the information specified in paragraph 14 … to the competent authorities of all other Member States …  
14.      The information to be communicated by the competent authority of a Member State under paragraph 13 shall contain the following, as applicable:  
(a)      the identification of intermediaries and relevant taxpayers, including their name, date and place of birth (in the case of an individual), residence for tax purposes, TIN and, where appropriate, the persons that are associated enterprises to the relevant taxpayer;  
(b)      details of the hallmarks set out in Annex IV that make the cross-border arrangement reportable;  
(c)      a summary of the content of the reportable cross-border arrangement, including a reference to the name by which it is commonly known, if any, and a description in abstract terms of the relevant business activities or arrangements, without leading to the disclosure of a commercial, industrial or professional secret or of a commercial process, or of information the disclosure of which would be contrary to public policy;  
(d)      the date on which the first step in implementing the reportable cross-border arrangement has been made or will be made;  
(e)      details of the national provisions that form the basis of the reportable cross-border arrangement;  
(f)      the value of the reportable cross-border arrangement;  
(g)      the identification of the Member State of the relevant taxpayer(s) and any other Member States which are likely to be concerned by the reportable cross-border arrangement;  
(h)      the identification of any other person in a Member State likely to be affected by the reportable cross-border arrangement, indicating to which Member States such person is linked.  
…’  
   
Belgian law  
7        The decreet betreffende de administratieve samenwerking op het gebied van belastingen (Decree on administrative cooperation in the field of taxation) of 21 June 2013 (  
Belgisch Staatsblad  
 of 26 June 2013, p. 40587; ‘the Decree of 21 June 2013’) transposes Directive 2011/16 in the Flemish Region (Belgium).  
8        That decree was amended by the decreet tot wijziging van het decreet van 21 juni 2013, wat betreft de verplichte automatische uitwisseling van inlichtingen op belastinggebied met betrekking tot meldingsplichtige grensoverschrijdende constructies (Decree amending the decree of 21 June 2013 as regards the mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements) of 26 June 2020 (  
Belgisch Staatsblad  
 of 3 July 2020, p. 49170; ‘the Decree of 26 June 2020’), which transposes Directive 2018/822.  
9        Subsection 2 of Section 2 of Chapter 2 of the Decree of 21 June 2013 governs the mandatory filing, by intermediaries or relevant taxpayers, of information on reportable cross-border tax arrangements.  
10      Article 11/6 of that subsection, as inserted into the Decree of 21 June 2013 by Article 14 of the Decree of 26 June 2020, defines the relationship between the reporting obligation and the legal professional privilege by which certain intermediaries are bound. It transposes Article 8ab(5) and (6) of amended Directive 2011/16. Paragraph 1 of that Article 11/6 provides:  
‘When an intermediary is bound by legal professional privilege, he or she is required:  
1°      to notify any other intermediary or intermediaries in writing, giving reasons, that he or she is unable to comply with the reporting obligation, as a result of which that reporting obligation automatically rests with the other intermediary or intermediaries;  
2°      in the absence of any other intermediary, to notify the relevant taxpayer or taxpayers of their reporting obligation, in writing, giving reasons.  
The waiver from the reporting obligation shall take effect only when an intermediary has fulfilled the obligation referred to in paragraph 1.’  
11      Article 11/7 of the Decree of 21 June 2013, as inserted into that decree by Article 15 of the Decree of 26 June 2020, states:  
‘… if the intermediary notifies the relevant taxpayer or another intermediary of the application of a waiver under Article 11/6(1), the obligation to file information on a reportable cross-border arrangement shall be incumbent on the other intermediary who has been notified, or if there is no such intermediary, the relevant taxpayer.’  
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
12      By applications of 31 August and 1 October 2020, the applicants in the main proceedings brought an action before the Grondwettelijk Hof (Constitutional Court, Belgium), which is the referring court, seeking suspension of the Decree of 26 June 2020 and its annulment in whole or in part.  
13      It is apparent from the order for reference that the applicants in the main proceedings dispute, in particular, the obligation provided for in the first subparagraph of Article 11/6(1) of the Decree of 21 June 2013, which was inserted into that decree by Article 14 of the Decree of 26 June 2020, which requires a lawyer acting as an intermediary, where he or she is bound by legal professional privilege, to inform the other intermediaries concerned in writing, stating reasons, that he or she cannot fulfil his or her reporting obligation. According to the applicants in the main proceedings, it is impossible to fulfil that obligation to provide information without infringing the legal professional privilege by which lawyers are bound. Furthermore, that obligation to provide information is not necessary in order to ensure that cross-border arrangements are reported, since the client, whether or not assisted by the lawyer, can him- or herself inform the other intermediaries and ask them to comply with their reporting obligation.  
14      The referring court notes that the information which lawyers must file with the competent authority with regard to their clients is protected by legal professional privilege, if that information relates to activities which fall within their specific tasks of defence or representation in legal proceedings and legal advice. It observes that the mere fact of having recourse to a lawyer is covered by legal professional privilege and that the same applies, a fortiori, as regards the identity of a lawyer’s client. Information protected by legal professional privilege vis-à-vis public authorities is also protected with regard to other actors, such as other intermediaries.  
15      The referring court states that, according to the   
travaux préparatoires  
 for the Decree of 26 June 2020, the obligation for an intermediary to inform other intermediaries, giving reasons, that he or she is subject to legal professional privilege and that he or she will not therefore fulfil the reporting obligation is required in order to satisfy the requirements of Directive 2018/822 and to ensure that legal professional privilege does not prevent the necessary reporting.  
16      That court notes that the actions in the main proceedings thus raise the question of the validity of Directive 2018/822, in so far as it has introduced such an obligation. Therefore, before a final ruling can be given on those actions, it is first necessary to resolve that question.  
17      In those circumstances, the Grondwettelijk Hof (Constitutional Court), first, ordered the suspension, inter alia, of the first subparagraph of Article 11/6(1) of the Decree of 21 June 2013, as inserted by Article 14 of the Decree of 26 June 2020, in so far as that provision imposes on a lawyer acting as an intermediary an obligation to provide information to another intermediary who is not his or her client, until the date of publication of the judgment ruling on those actions. Second, that court decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
‘Does Article 1(2) of [Directive 2018/822] infringe the right to a fair trial as guaranteed by Article 47 of the [Charter] and the right to respect for private life as guaranteed by Article 7 of the [Charter], in that the new Article 8ab(5) which it inserted in [Directive 2011/16], provides that, where a Member State takes the necessary measures to give intermediaries the right to waiver from filing information on a reportable cross-border arrangement where the reporting obligation would breach the legal professional privilege under the national law of that Member State, that Member State is obliged to require the intermediaries to notify, without delay, any other intermediary or, if there is no such intermediary, the relevant taxpayer, of their reporting obligations, in so far as the effect of that obligation is to oblige a lawyer acting as an intermediary to share with another intermediary, not being his [or her] client, information which he [or she] obtains in the course of the essential activities of his [or her] profession, namely, representing or defending clients in legal proceedings and giving legal advice, even in the absence of pending legal proceedings?’  
   
Consideration of the question referred  
18      As a preliminary point, it should be noted that, although the question put refers to the obligation to notify, laid down in Article 8ab(5) of amended Directive 2011/16, both with regard to intermediaries and, in the absence of any intermediary, to the relevant taxpayer, it is nevertheless apparent from reading the request for a preliminary ruling as a whole that the referring court is in fact seeking to ascertain only the validity of that obligation in so far as the notification must be made, by a lawyer acting as an intermediary (‘the lawyer-intermediary’), within the meaning of Article 3(21) of that directive, to another intermediary who is not his or her client.  
19      Where the notification provided for in Article 8ab(5) of amended Directive 2011/16 is made by the lawyer-intermediary to his or her client, whether that client is another intermediary or the relevant taxpayer, that notification is not capable of calling into question respect for the rights and freedoms guaranteed by Articles 7 and 47 of the Charter on account, first, of the absence of any obligation of legal professional privilege on the part of the lawyer-intermediary vis-à-vis his or her client and, second, of the fact that, at the stage of the execution by that client of his or her reporting obligations under that directive, the confidentiality of the relationship between the lawyer-intermediary and that client precludes the latter from being required to reveal to third parties and, in particular, to the tax authorities, that he or she has consulted a lawyer.  
20      It is thus apparent from the order for reference that, by its question, the referring court asks the Court, in essence, to examine the validity, in the light of Articles 7 and 47 of the Charter, of Article 8ab(5) of amended Directive 2011/16, in so far as the Member States’ application of that provision has the effect of requiring a lawyer acting as an intermediary, within the meaning of Article 3(21) of that directive, where he or she is exempt from the reporting obligation laid down in paragraph 1 of Article 8ab of that directive on account of the legal professional privilege by which he or she is bound, to notify without delay any other intermediary who is not his or her client of that intermediary’s reporting obligations under paragraph 6 of that Article 8ab.  
21      In that regard, it must be borne in mind that, in accordance with Article 8ab(1) of amended Directive 2011/16, each Member State is to take the necessary measures to require intermediaries to file information that is within their knowledge, possession or control on reportable cross-border arrangements with the competent authorities within 30 days. The reporting obligation laid down in that provision applies to all reportable cross-border arrangements and, therefore, both to bespoke arrangements, defined in Article 3(25) of amended Directive 2011/16, and marketable arrangements, defined in Article 3(24) thereof.  
22      It should be noted that lawyers may, in the performance of their activities, be ‘intermediaries’ within the meaning of Article 3(21) of amended Directive 2011/16, by reason of the fact that they may themselves perform activities relating to designing, marketing, organising, making available for implementation or managing the implementation of reportable cross-border arrangements or, failing that, because they may provide aid, assistance or advice in relation to such activities. Lawyers carrying out such activities are thus, in principle, subject to the reporting obligation laid down in Article 8ab(1) of that directive.  
23      However, under the first subparagraph of Article 8ab(5) of amended Directive 2011/16, each Member State may take the necessary measures to give intermediaries, and in particular lawyer-intermediaries, a waiver from filing information on a reportable cross-border arrangement where the reporting obligation would breach the legal professional privilege under the law of that Member State. In such circumstances, each Member State is to take the necessary measures to require intermediaries to notify, without delay, any other intermediary or, if there is no such intermediary, the relevant taxpayer of their reporting obligations under paragraph 6 of that article. That paragraph provides that, in such a case, the reporting obligation lies with the other notified intermediary or, if there is no such intermediary, with the relevant taxpayer.  
24      It must nevertheless be pointed out that, under the second subparagraph of Article 8ab(5) of amended Directive 2011/16, intermediaries may only be entitled to a waiver under the first subparagraph thereof to the extent that they operate within the limits of the relevant national laws that define their profession, which it is, where relevant, for the national court to ascertain when applying that legislation. Therefore, it is only in relation to lawyer-intermediaries who actually operate within such limits that the validity of Article 8ab(5) of that directive must be examined in the light of Articles 7 and 47 of the Charter.  
25      In that regard, it should be noted that Article 7 of the Charter, which recognises that everyone has the right to respect for his or her private and family life, home and communications, corresponds to Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (‘the ECHR’), while Article 47, which guarantees the right to an effective remedy and the right to a fair trial, corresponds to Article 6(1) ECHR.  
26      In accordance with Article 52(3) of the Charter, which is intended to ensure the necessary consistency between the rights contained in the Charter and the corresponding rights guaranteed in the ECHR, without adversely affecting the autonomy of EU law, the Court must therefore take into account, when interpreting the rights guaranteed by Articles 7 and 47 of the Charter, the corresponding rights guaranteed by Article 8(1) and Article 6(1) ECHR, as interpreted by the European Court of Human Rights (‘the ECtHR’), as the minimum threshold of protection (see, to that effect, judgment of 2 February 2021,   
Consob  
, C-481/19, EU:C:2021:84, paragraphs 36 and 37).  
27      As regards the validity of Article 8ab(5) of amended Directive 2011/16 in the light of Article 7 of the Charter, it is apparent from the case-law of the ECtHR that Article 8(1) ECHR protects the confidentiality of all correspondence between individuals and affords strengthened protection to exchanges between lawyers and their clients (see, to that effect, ECtHR, judgment of 6 December 2012,   
Michaud v. France  
, CE:ECHR:2012:1206JUD001232311, §§ 117 and 118). Like that provision, the protection of which covers not only the activity of defence but also legal advice, Article 7 of the Charter necessarily guarantees the secrecy of that legal consultation, both with regard to its content and to its existence. As the ECtHR has pointed out, individuals who consult a lawyer can reasonably expect that their communication is private and confidential (ECtHR, judgment of 9 April 2019,   
Altay v. Turkey   
(No 2)  
, CE:ECHR:2019:0409JUD001123609, § 49). Therefore, other than in exceptional situations, those persons must have a legitimate expectation that their lawyer will not disclose to anyone, without their consent, that they are consulting him or her.  
28      The specific protection which Article 7 of the Charter and Article 8(1) ECHR afford to lawyers’ legal professional privilege, which primarily takes the form of obligations on them, is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants (ECtHR, judgment of 6 December 2012,   
Michaud v. France  
, CE:ECHR:2012:1206JUD001232311, §§ 118 and 119). That fundamental task entails, on the one hand, the requirement, the importance of which is recognised in all the Member States, that any person must be able, without constraint, to consult a lawyer whose profession encompasses, by its very nature, the giving of independent legal advice to all those in need of it and, on the other, the correlative duty of the lawyer to act in good faith towards his or her client (see, to that effect, judgment of 18 May 1982,   
AM & S Europe   
v  
 Commission  
, 155/79, EU:C:1982:157, paragraph 18).  
29      The obligation laid down by Article 8ab(5) of amended Directive 2011/16 for a lawyer-intermediary where he or she is, on account of the legal professional privilege by which he or she is bound by national law, exempt from the reporting obligation laid down in Article 8ab(1) to notify without delay other intermediaries who are not his or her clients of their reporting obligations under Article 8ab(6) of that directive, necessarily entails the consequence that those other intermediaries become aware of the identity of the notifying lawyer-intermediary, of his or her assessment that the arrangement at issue is reportable and of his or her having been consulted in connection with the arrangement.  
30      In those circumstances and in so far as those other intermediaries do not necessarily have knowledge of the identity of the lawyer-intermediary and of his or her having been consulted on the reportable cross-border arrangement, the obligation to notify, laid down in Article 8ab(5) of amended Directive 2011/16, entails an interference with the right to respect for communications between lawyers and their clients, guaranteed in Article 7 of the Charter.  
31      Furthermore, it must be observed that that obligation to notify leads, indirectly, to another interference with that right, resulting from the disclosure, by the third-party intermediaries thus notified, to the tax authorities of the identity of the lawyer-intermediary and of his or her having been consulted.  
32      It is apparent from Article 8ab(1), (9), (13) and (14) of amended Directive 2011/16 that the identification of the intermediaries is one of the items of information to be provided pursuant to the reporting obligation, that identification being the subject of an exchange of information between the competent authorities of the Member States. Consequently, in the event of notification under Article 8ab(5) of that directive, the third-party intermediaries notified, who are thus informed of the identity of the lawyer-intermediary and of his or her having been consulted in connection with the reportable cross-border arrangement and who are not themselves bound by legal professional privilege, must inform the competent authorities referred to in Article 3(1) of that directive not only of the existence of that arrangement and of the identity of the relevant taxpayer or taxpayers, but also of the identity of the lawyer-intermediary and of his or her having been consulted.  
33      Accordingly, it is necessary to examine whether those interferences with the right to respect for communications between lawyers and their clients, guaranteed in Article 7 of the Charter, may be justified.  
34      In that context, it must be recalled that the rights enshrined in Article 7 of the Charter are not absolute rights, but must be considered in relation to their function in society. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (see, to that effect, judgment of 6 October 2020,   
Privacy International  
, C-623/17, EU:C:2020:790, paragraphs 63 and 64).   
35      In the first place, as regards the requirement that any limitation on the exercise of fundamental rights must be provided for by law, this implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned, bearing in mind, on the one hand, that that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances. On the other hand, the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter (judgment of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraph 114 and the case-law cited).  
36      In that regard, it should be noted that, first, paragraph 5 of Article 8ab of amended Directive 2011/16 expressly lays down the obligation, for a lawyer-intermediary who is exempt from the obligation to file information on account of the legal professional privilege by which he or she is bound, to notify other intermediaries of their reporting obligations under paragraph 6 of that Article 8ab. Second, as has been found in paragraphs 29 and 30 of the present judgment, the interference with the right to respect for communications between lawyers and their clients, enshrined in Article 7 of the Charter, is the direct consequence of such notification by the lawyer to another intermediary who is not his or her client, in particular where that client was not aware, up to the time of that notification, of the identity of that lawyer and of the latter’s having been consulted on the reportable cross-border arrangement.  
37      Furthermore, as regards the interference resulting indirectly from that obligation to notify on account of the disclosure, by the notified third-party intermediaries, of the identity of the lawyer-intermediary and of his or her having been consulted to the tax authorities, that disclosure is due, as has been found in paragraphs 31 and 32 of the present judgment, to the extent of the obligations to provide information flowing from Article 8ab(1), (9), (13) and (14) of amended Directive 2011/16.  
38      In those circumstances, the principle of legality must be considered to have been fulfilled.  
39      In the second place, as regards respect for the essence of the right to respect for communications between lawyers and their clients, guaranteed in Article 7 of the Charter, it should be noted that the obligation to notify, established by Article 8ab(5) of amended Directive 2011/16, entails only to a limited extent the lifting, vis-à-vis a third-party intermediary and the tax authorities, of the confidentiality of the communications between the lawyer-intermediary and his or her client. In particular, that provision does not provide for an obligation, or even authorisation, for the lawyer-intermediary to share, without his or her client’s consent, information on the content of those communications with other intermediaries and those intermediaries will therefore not be in a position to file such information with the tax authorities.  
40      In those circumstances, it cannot be held that the obligation to notify laid down in Article 8ab(5) of amended Directive 2011/16 undermines the essence of the right to respect for communications between lawyers and their clients enshrined in Article 7 of the Charter.  
41      In the third place, as regards observance of the principle of proportionality, that principle requires that the limitations which may, in particular, be imposed by acts of EU law on rights and freedoms enshrined in the Charter do not exceed the limits of what is appropriate and necessary in order to meet the legitimate objectives pursued or the need to protect the rights and freedoms of others; where there is a choice between several appropriate measures, recourse must be had to the least onerous. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue, in order to ensure that the disadvantages caused by that measure are not disproportionate to the aims pursued. Thus, the possibility of Member States justifying a limitation of the rights guaranteed in Article 7 of the Charter must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness (judgments of 26 April 2022,   
Poland   
v  
 Parliament and Council  
, C-401/19, EU:C:2022:297, paragraph 65, and of 22 November 2022,   
Luxembourg Business Registers and Sovim  
, C-37/20 and C-601/20, EU:C:2022:912, paragraph 64).  
42      Therefore, it is necessary to ascertain, first of all, whether the reporting obligation laid down in Article 8ab(5) of amended Directive 2011/16 meets an objective of general interest recognised by the European Union. If so, it must then be ensured, first, that the obligation is appropriate for attaining that objective, secondly, that the interference with the fundamental right to respect for communications between lawyers and their clients which may result from that obligation to notify is limited to what is strictly necessary, in the sense that the objective pursued could not reasonably be achieved in an equally effective manner by other means less prejudicial to that right, and, thirdly, provided that that is indeed the case, that that interference is not disproportionate to that objective, which implies, in particular, a balancing of the importance of the objective and the seriousness of the interference (see, to that effect, judgment of 22 November 2022,   
Luxembourg Business Registers and Sovim  
, C-37/20 and C-601/20, EU:C:2022:912, paragraph 66).  
43      As the Advocate General observed in point 88 of his Opinion, the amendment made to Directive 2011/16 by Directive 2018/822 falls within the scope of international tax cooperation to combat aggressive tax planning, manifested by the exchange of information between Member States. In that regard, it is apparent in particular from recitals 2, 4, 8 and 9 of Directive 2018/822 that the reporting and notification obligations established by Article 8ab of amended Directive 2011/16 are intended to contribute to the prevention of the risk of tax avoidance and evasion.  
44      Combating aggressive tax planning and preventing the risk of tax avoidance and evasion constitute objectives of general interest recognised by the European Union for the purposes of Article 52(1) of the Charter, capable of enabling a limitation to be placed on the exercise of the rights guaranteed by Article 7 of the Charter (see, to that effect, judgment of 6 October 2020,   
État luxembourgeois (Right to bring an action against a request for information in tax matters)  
, C-245/19 and C-246/19, EU:C:2020:795, paragraph 87).  
45      As regards the question whether the obligation to notify laid down in Article 8ab(5) of amended Directive 2011/16 is appropriate and necessary for the attainment of those objectives, the French and Latvian Governments maintain, in essence, that such notification makes it possible, inter alia, to raise awareness among other intermediaries of their duty to comply with the reporting obligation and thus to avoid the possibility that those other intermediaries are not informed of the fact that the obligation to report the cross-border arrangement has been transferred to them pursuant to Article 8ab(6) of amended Directive 2011/16. Therefore, according to those governments, in the absence of an obligation on the lawyer-intermediary to notify, there is a risk that the cross-border arrangement will not be declared at all, contrary to the objectives pursued by that directive.  
46      Even if the notification obligation established by Article 8ab(5) of amended Directive 2011/16 is indeed capable of contributing to the combating of aggressive tax planning and the prevention of the risk of tax avoidance and evasion, it must be held that that obligation cannot, however, be regarded as being strictly necessary in order to attain those objectives and, in particular, to ensure that the information concerning the reportable cross-border arrangements is filed with the competent authorities.  
47      First, intermediaries’ reporting obligations are clearly set out in amended Directive 2011/16, in particular in Article 8ab(1) thereof. Under that provision, all intermediaries are, in principle, required to file information that is within their knowledge, possession or control on reportable cross-border arrangements with the competent authorities. In addition, in accordance with the first subparagraph of Article 8ab(9) of that directive, each Member State is to take the necessary measures to require that, where there is more than one intermediary, the obligation to file information lie with all intermediaries involved in the same reportable cross-border arrangement. No intermediary can therefore usefully argue that he or she was unaware of the reporting obligations to which he or she is directly and individually subject, merely because he or she is an intermediary.  
48      Secondly, as regards the Latvian Government’s argument that the obligation to notify reduces the risk that other intermediaries would rely on the fact that the lawyer-intermediary will report the required information to the competent authorities and that they will refrain for that reason from themselves making such a report, it should be noted, on the one hand, that, in so far as the consultation of a lawyer is subject to legal professional privilege, other intermediaries will not, as has been pointed out in paragraph 30 of the present judgment, necessarily be aware of the identity of the lawyer-intermediary and of his or her having been consulted concerning the reportable cross-border arrangement, which in such circumstances precludes such a risk from the outset.  
49      On the other hand, even in the opposite situation in which other intermediaries have such awareness, there is no reason to fear that they would rely, without verification, on the lawyer-intermediary making the required report, since the second subparagraph of Article 8ab(9) of amended Directive 2011/16 specifies that an intermediary is to be exempt from filing the information only on condition that it has proof that the same information has already been filed by another intermediary. Furthermore, by expressly providing, in Article 8ab(5) thereof, that legal professional privilege may lead to a waiver from the reporting obligation, amended Directive 2011/16 makes a lawyer-intermediary a person from whom other intermediaries cannot, a priori, expect any initiative capable of relieving them of their own reporting obligations.  
50      Thirdly, it should be borne in mind that any intermediary who, because of the legal professional privilege by which he or she is bound by national law, is exempt from the reporting obligation laid down in paragraph 1 of Article 8ab of amended Directive 2011/16 is nevertheless still required to notify without delay his or her client of his or her reporting obligations under paragraph 6 of that provision.  
51      Fourthly, as regards the disclosure, by notified third-party intermediaries, of the identity of the lawyer-intermediary and of his or her having been consulted to the tax authorities, that disclosure also does not appear to be strictly necessary for the pursuit of the objectives of amended Directive 2011/16 of combating aggressive tax planning and preventing the risk of tax avoidance and evasion.  
52      On the one hand, the reporting obligation on other intermediaries not subject to legal professional privilege and, if there are no such intermediaries, that obligation on the relevant taxpayer ensure, in principle, that the tax authorities are informed of reportable cross-border arrangements. In addition, the tax authorities may, after receiving such information, request, if necessary, additional information relating to the arrangement in question directly from the relevant taxpayer, who will then be able to consult his or her lawyer for assistance, or they may conduct an audit of that taxpayer’s tax situation.  
53      On the other hand, in view of the reporting waiver in Article 8ab(5) of amended Directive 2011/16, the disclosure to the tax authorities of the identity of the lawyer-intermediary and of his or her having been consulted will not, in any event, enable those authorities to require that lawyer-intermediary to provide information without the consent of his or her client.  
54      At the hearing before the Court, the Commission submitted, however, in essence, that the disclosure of the identity of the lawyer-intermediary and of his or her having been consulted would be necessary in order to enable the tax authorities to ascertain whether that lawyer-intermediary is justified in relying on legal professional privilege.  
55      That argument cannot be accepted.  
56      It is true that, as has been pointed out in paragraph 24 of the present judgment, the second subparagraph of paragraph 5 of Article 8ab of amended Directive 2011/16 specifies that lawyer-intermediaries may only be entitled to a waiver under the first subparagraph of that provision to the extent that they operate within the limits of the relevant national laws that define their profession. However, the purpose of the reporting and notification obligations laid down in Article 8ab of that directive is not to check that lawyer-intermediaries operate within those limits, but to combat potentially aggressive tax practices and to prevent the risk of tax avoidance and evasion, by ensuring that the information concerning the reportable cross-border arrangements is filed with the competent authorities.  
57      As is apparent from paragraphs 47 to 53 of the present judgment, that directive ensures that such information is provided to the tax authorities, without the disclosure to them of the identity of the lawyer-intermediary and of his or her having been consulted being necessary for that purpose.  
58      In those circumstances, the possibility that lawyer-intermediaries might wrongly rely on legal professional privilege in order to avoid their reporting obligation cannot permit the inference that the obligation to notify laid down in Article 8ab(5) of that directive and the disclosure to the tax authorities of the identity and consultation of the notifying lawyer-intermediary which is the consequence thereof are strictly necessary.  
59      It follows from the foregoing considerations that Article 8ab(5) of amended Directive 2011/16 infringes the right to respect for communications between a lawyer and his or her client, guaranteed in Article 7 of the Charter, in so far as it provides, in essence, that a lawyer-intermediary, who is subject to legal professional privilege, is required to notify any other intermediary who is not his or her client of that other intermediary’s reporting obligations.  
60      As regards the validity of Article 8ab(5) of amended Directive 2011/16 in the light of Article 47 of the Charter, it must be recalled that the right to a fair trial, guaranteed by that provision, consists of various elements. It includes, inter alia, the rights of the defence, the principle of equality of arms, the right of access to the courts and the right of access to a lawyer, both in civil and criminal proceedings. Lawyers would be unable to carry out satisfactorily their task of advising, defending and representing their clients, who would in consequence be deprived of the rights conferred on them by Article 47 of the Charter, if lawyers were obliged, in the context of judicial proceedings or the preparation for such proceedings, to cooperate with the authorities by passing them information obtained in the course of related legal consultations (see, to that effect, judgment of 26 June 2007,   
Ordre des barreaux francophones et germanophones and Others  
, C-305/05, EU:C:2007:383, paragraphs 31 and 32).  
61      It follows from those considerations that the requirements implied by the right to a fair trial presuppose, by definition, a link with judicial proceedings (see, to that effect, judgment of 26 June 2007,   
Ordre des barreaux francophones et germanophones and Others  
, C-305/05, EU:C:2007:383, paragraph 35).  
62      However, it must be stated that such a link has not been established in the present case.  
63      It follows from Article 8ab(1) and (5) of amended Directive 2011/16, and in particular from the time limits laid down in those provisions, that the obligation to notify arises at an early stage, at the latest when the reportable cross-border arrangement has just been finalised and is ready to be implemented, and thus outside the framework of legal proceedings or their preparation.  
64      As the Advocate General observed, in essence, in point 41 of his Opinion, at that early stage, the lawyer-intermediary is not acting as the defence counsel for his or her client in a dispute and the mere fact that the lawyer’s advice or the cross-border arrangement which is the subject of his or her consultation may give rise to litigation at a later stage does not mean that the lawyer acted for the purposes and in the interests of the rights of defence of his or her client.  
65      In those circumstances, it must be held that the obligation to notify replacing, for the lawyer-intermediary bound by legal professional privilege, the reporting obligation laid down in Article 8ab(1) of amended Directive 2011/16 does not entail any interference with the right to a fair trial, guaranteed in Article 47 of the Charter.  
66      It follows from all the foregoing considerations that the answer to the question referred is that Article 8ab(5) of amended Directive 2011/16 is invalid in the light of Article 7 of the Charter, in so far as the Member States’ application of that provision has the effect of requiring a lawyer acting as an intermediary, within the meaning of Article 3(21) of that directive, where he or she is exempt from the reporting obligation laid down in paragraph 1 of Article 8ab of that directive on account of the legal professional privilege by which he or she is bound, to notify without delay any other intermediary who is not his or her client of that intermediary’s reporting obligations under paragraph 6 of that Article 8ab.  
   
Costs  
67      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
Article 8ab(5) of Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, as amended by Council Directive (EU) 2018/822 of 25 May 2018, is invalid in the light of Article 7 of the Charter of Fundamental Rights of the European Union, in so far as the Member States’ application of that provision has the effect of requiring a lawyer acting as an intermediary, within the meaning of Article 3(21) of that directive, as amended, where he or she is exempt from the reporting obligation laid down in paragraph 1 of Article 8ab of that directive, as amended, on account of the legal professional privilege by which he or she is bound, to notify without delay any other intermediary who is not his or her client of that intermediary’s reporting obligations under paragraph 6 of that Article 8ab.

ID: 02bddaff-98c7-441a-9118-954b4cc78920

Judgment of 20 Dec 2017, C-434/16 (  
Peter Nowak v Data Protection Commissioner  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to rectification   
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accuracy   
   
JUDGMENT OF THE COURT (Second Chamber)  
20 December 2017 (\*)  
(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Article 2(a) — Concept of ‘personal data’ — Written answers submitted by a candidate in a professional examination — Examiner’s comments with respect to those answers — Article 12(a) and (b) — Extent of the data subject’s rights to access and rectification)  
In Case C-434/16,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Supreme Court (Ireland), made by decision of 29 July 2016, received at the Court on 4 August 2016, in the proceedings  
Peter Nowak  
v  
Data Protection Commissioner,  
THE COURT (Second Chamber),  
composed of M. Ilešič (Rapporteur), President of the Chamber, A. Rosas, C. Toader, A. Prechal, and E. Jarašiūnas, Judges,  
Advocate General: J. Kokott,  
Registrar: M. Aleksejev, Administrator,  
having regard to the written procedure and further to the hearing on 22 June 2017,  
after considering the observations submitted on behalf of:  
–        Mr Nowak, by G. Rudden, Solicitor, and N. Travers, Senior Counsel,  
–        the Data Protection Commissioner, by D. Young, Solicitor, and P.A. McDermott, Senior Counsel,  
–        Ireland, by E. Creedon, L. Williams and A. Joyce, acting as Agents, and by A. Caroll, Barrister,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the Greek Government, by G. Papadaki and S. Charitaki, acting as Agents,  
–        the Hungarian Government, by Z. Fehér and A. Pálfy, acting as Agents,  
–        the Austrian Government, by G. Eberhard, acting as Agent,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes, M. Figueiredo and I. Oliveira, acting as Agents,  
–        the European Commission, by D. Nardi and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 20 July 2017,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Mr Peter Nowak and the Data Protection Commissioner (Ireland) concerning the latter’s refusal to give Mr Nowak access to a corrected script of an examination at which he was a candidate, on the ground that the information contained therein did not constitute personal data.  
   
Legal context  
   
European Union law  
 Directive 95/46  
3        Recitals 25, 26 and 41 of Directive 95/46, the object of which is stated in Article 1 thereof to be the protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and the elimination of obstacles to the free flow of such data, state:  
‘(25)      … the principles of protection must be reflected, on the one hand, in the obligations imposed on persons … responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;  
(26)      … the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; … the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; ...  
...  
(41)      … any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing;’  
4        The concept of ‘personal data’ is defined in Article 2(a) of that directive as being ‘any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’.  
5        Article 6 of that directive, within Section I of Chapter II of that directive, that section being headed ‘Principles relating to data quality’, is worded as follows:  
‘1.      Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
6        Article 7 of Directive 95/46, within Section II of Chapter II of that directive, that section being headed ‘Criteria for making data processing legitimate’, provides:   
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent; or  
...  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject; or  
...  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
7        Article 12 of that directive, headed ‘Right of access’, states:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
(a)      without constraint at reasonable intervals and without excessive delay or expense:  
–        confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,  
–        communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,  
...  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
(c)      notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.’  
8        Article 13 of that directive, headed ‘Exemptions and restrictions’, provides:  
‘1.      Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:  
...  
(g)      the protection of the data subject or of the rights and freedoms of others.  
...’  
9        Article 14 of Directive 95/46, headed ‘The data subject’s right to object’, provides:  
‘Member States shall grant the data subject the right:  
(a)      at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;  
...’  
10      Article 28 of that directive, headed ‘Supervisory authority’, states:  
‘1.      Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.  
...  
3.      Each authority shall in particular be endowed with:  
–        investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;  
–        effective powers of intervention, such as, for example, that … of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing …  
...  
Decisions by the supervisory authority, which give rise to complaints, may be appealed against through the courts.  
4.      Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.  
...’  
 Regulation (EU) 2016/679  
11      Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) is applicable, pursuant to Article 99(2) thereof, as from 25 May 2018. Article 94(1) of that regulation provides that Directive 95/46 is repealed with effect from that date.   
12      Article 15 of that regulation, headed ‘Right of access by the data subject’, provides:  
‘1.      The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data …  
...  
3.      The controller shall provide a copy of the personal data undergoing processing …  
4.      The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.’  
13      Article 23 of Regulation 2016/679, headed ‘Restrictions’, states:   
‘1.      Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 …, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
...  
(e)      other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;  
...  
(i)      the protection of the data subject or of the rights and freedoms of others.  
...’  
   
Irish law  
14      The Data Protection Act 1988, as amended by the Data Protection (Amendment) Act 2003 (‘the data protection legislation’) is designed to transpose Directive 95/46 into the Irish legal system. Section 1(1) of that Act defines the concept of ‘personal data’ as follows:  
‘Data relating to a living individual who is or can be identified either from the data or from data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller’.  
15      The right of access is governed by Section 4 of the data protection legislation; Section 4(6), which relates specifically to requests for access to the results of examinations, is worded as follows:  
‘(a)      A request by an individual under subsection (1) of this section in relation to the results of an examination at which he was a candidate shall be deemed, for the purposes of this section, to be made on   
(i)      the date of the first publication of the results of the examination, or   
ii)      the date of the request,   
whichever is the later; ...  
(b)      In this subsection “examination” means any process for determining the knowledge, intelligence, skill or ability of a person by reference to his performance in any test, work or other activity.’  
16      Article 6 of the data protection legislation establishes the right to rectification and erasure of personal data the processing of which does not comply with that legislation.   
17      Article 10(1)(b)(i) of the data protection legislation requires the Data Protection Commissioner to investigate a complaint ‘unless he is of the opinion that it is frivolous or vexatious’.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
18      Mr Nowak was a trainee accountant who passed first level accountancy examinations and three second level examinations set by the Institute of Chartered Accountants of Ireland (‘the CAI’). However, Mr Nowak failed the Strategic Finance and Management Accounting examination, which allowed candidates to make use of documents (an open book examination).   
19      After he had failed that examination for the fourth time, in the autumn of 2009, Mr Nowak initially submitted a challenge to the result of that examination. After that challenge was rejected in March 2010, he submitted, in May 2010, a data access request, under Section 4 of the data protection legislation, seeking all the personal data relating to him held by the CAI.  
20      By letter of 1 June 2010, the CAI sent 17 documents to Mr Nowak, but refused to send to him his examination script, on the ground that it did not contain personal data, within the meaning of the data protection legislation.  
21      Mr Nowak then contacted the Data Protection Commissioner with a view to challenging the reason given for the refusal to disclose his examination script. In June 2010 the Data Protection Commissioner replied to him by email to state, inter alia, that ‘exam scripts do not generally fall to be considered [for data protection purposes] … because this material would not generally constitute personal data’.  
22      That reply from the Data Protection Commissioner was followed by correspondence between Mr Nowak and the Commissioner which culminated, on 1 July 2010, in Mr Nowak submitting a formal complaint.   
23      By letter of 21 July 2010, the Data Protection Commissioner informed Mr Nowak that, after consideration of the case, he had identified no substantive contravention of [the data protection legislation] and that, in accordance with Section 10(1)(b)(i) of that legislation, which covers frivolous or vexatious complaints, there would be no investigation of the complaint. The letter stated, further, that the material over which Mr Nowak sought to exercise ‘a right of correction is not personal data to which Section 6 of the [data protection legislation] applies’.  
24      Mr Nowak brought an action against that decision before the Circuit Court. That court held that the action was inadmissible on the ground that, since the Data Protection Commissioner had not initiated an investigation of a complaint, there was no decision against which legal proceedings could be brought. In the alternative, that court held that the action was unfounded, since the examination script did not constitute personal data.  
25      Mr Nowak brought an appeal against the judgment of that court before the High Court, which however upheld the decision. The judgment of the High Court was, in its turn, upheld by the Court of Appeal. The Supreme Court, which allowed an appeal against the judgment of the Court of Appeal, held that the action brought by Mr Nowak against the decision of the Data Protection Commissioner was admissible.  
26      However, the Supreme Court is uncertain whether an examination script can constitute personal data, within the meaning of Directive 95/46, and therefore decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:  
‘(1)      Is information recorded in/as answers given by a candidate during a professional examination capable of being personal data, within the meaning of Directive 95/46?  
(2)      If the answer to Question 1 is that all or some of such information may be personal data within the meaning of the Directive, what factors are relevant in determining whether in any given case such script is personal data, and what weight should be given to such factors?’  
   
Consideration of the questions referred  
27      By its questions, which can be examined together, the referring court seeks, in essence, to ascertain whether Article 2(a) of Directive 95/46 must be interpreted as meaning that, in circumstances such as those at issue in the main proceedings, the written answers submitted by a candidate at a professional examination and any examiner’s comments with respect to those answers constitute personal data, within the meaning of that provision.  
28      In that regard, it must be recalled that Article 2(a) of Directive 95/46 defines personal data as meaning ‘any information relating to an identified or identifiable natural person’. Under the same provision, ‘an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’.  
29      It is not disputed that a candidate at a professional examination is a natural person who can be identified, either directly, through his name, or indirectly, through an identification number, these being placed either on the examination script itself or on its cover sheet.   
30      Contrary to what the Data Protection Commissioner appears to argue, it is of no relevance, in that context, whether the examiner can or cannot identify the candidate at the time when he/she is correcting and marking the examination script.   
31      For information to be treated as ‘personal data’ within the meaning of Article 2(a) of Directive 95/46, there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person (judgment of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 43). It is also undisputed that, in the event that the examiner does not know the identity of the candidate when he/she is marking the answers submitted by that candidate in an examination, the body that set the examination, in this case the CAI, does, however, have available to it the information needed to enable it easily and infallibly to identify that candidate through his identification number, placed on the examination script or its cover sheet, and thereby to ascribe the answers to that candidate.   
32      It is however necessary to determine whether the written answers provided by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute information relating to that candidate, within the meaning of Article 2(a) of Directive 95/46.   
33      As the Court has held previously, the scope of Directive 95/46 is very wide and the personal data covered by that directive is varied (judgment of 7 May 2009,   
Rijkeboer  
, C-553/07, EU:C:2009:293, paragraph 59 and the case-law cited).  
34      The use of the expression ‘any information’ in the definition of the concept of ‘personal data’, within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it ‘relates’ to the data subject.   
35      As regards the latter condition, it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person.  
36      As is argued, in essence, by Mr Nowak, the Czech, Greek, Hungarian, Austrian and Portuguese governments and also by the European Commission, the written answers submitted by a candidate at a professional examination constitute information that is linked to him or her as a person.  
37      First, the content of those answers reflects the extent of the candidate’s knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment. In the case of a handwritten script, the answers contain, in addition, information as to his handwriting.   
38      Second, the purpose of collecting those answers is to evaluate the candidate’s professional abilities and his suitability to practice the profession concerned.   
39      Last, the use of that information, one consequence of that use being the candidate’s success or failure at the examination concerned, is liable to have an effect on his or her rights and interests, in that it may determine or influence, for example, the chance of entering the profession aspired to or of obtaining the post sought.  
40      It is, moreover, equally true that the written answers submitted by a candidate at a professional examination constitute information that relates to that candidate by reason of its content, purpose or effect, where the examination is, as in this case, an open book examination.   
41      As is stated by the Advocate General in point 24 of her Opinion, the aim of any examination is to determine and establish the individual performance of a specific person, namely the candidate, and not, unlike, for example, a representative survey, to obtain information that is independent of that person.   
42      As regards the comments of an examiner with respect to the candidate’s answers, it is clear that they, no less than the answers submitted by the candidate at the examination, constitute information relating to that candidate.   
43      The content of those comments reflects the opinion or the assessment of the examiner of the individual performance of the candidate in the examination, particularly of his or her knowledge and competences in the field concerned. The purpose of those comments is, moreover, precisely to record the evaluation by the examiner of the candidate’s performance, and those comments are liable to have effects for the candidate, as stated in paragraph 39 of this judgment.   
44      The finding that the comments of the examiner with respect to the answers submitted by the candidate at the examination constitute information which, by reason of its content, purpose or effect, is linked to that candidate is not called into question by the fact that those comments also constitute information relating to the examiner.   
45      The same information may relate to a number of individuals and may constitute for each of them, provided that those persons are identified or identifiable, personal data, within the meaning of Article 2(a) of Directive 95/46.   
46      Further, the question whether written answers submitted by a candidate at a professional examination and any comments made by the examiner with respect to those answers should be classified as personal data cannot be affected, contrary to what is argued by the Data Protection Commissioner and the Irish government, by the fact that the consequence of that classification is, in principle, that the candidate has rights of access and rectification, pursuant to Article 12(a) and (b) of Directive 95/46.  
47      In that regard, it must, first, be recalled, as argued by the Commission at the hearing, that a number of principles and safeguards, provided for by Directive 95/46, are attached to that classification and follow from that classification.   
48      It is stated in recital 25 of Directive 95/46 that the principles of protection provided for by that directive are reflected, on the one hand, in the obligations imposed on those responsible for processing data, obligations which concern in particular data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.   
49      Accordingly, if information relating to a candidate, contained in his or her answers submitted at a professional examination and in the comments made by the examiner with respect to those answers, were not to be classified as ‘personal data’, that would have the effect of entirely excluding that information from the obligation to comply not only with the principles and safeguards that must be observed in the area of personal data protection, and, in particular, the principles relating to the quality of such data and the criteria for making data processing legitimate, established in Articles 6 and 7 of Directive 95/46, but also with the rights of access, rectification and objection of the data subject, provided for in Articles 12 and 14 of that directive, and with the supervision exercised by the supervisory authority under Article 28 of that directive.   
50      As stated by the Advocate General in point 26 of her Opinion, it is undisputed that an examination candidate has, inter alia, a legitimate interest, based on the protection of his private life, in being able to object to the processing of the answers submitted by him at that examination and of the examiner’s comments with respect to those answers outside the examination procedure and, in particular, to their being sent to third parties, or published, without his permission. Equally, the body setting the examination, as the data controller, is obliged to ensure that those answers and comments are stored in such a way as to ensure that third parties do not have unlawful access to them.   
51      Further, it is clear that the rights of access and rectification, provided for in Article 12(a) and (b) of Directive 95/46, may also be asserted in relation to the written answers submitted by a candidate at a professional examination and to any comments made by an examiner with respect to those answers.  
52      Of course, the right of rectification provided for in Article 12(b) of Directive 95/46 cannot enable a candidate to ‘correct’,   
a posteriori  
, answers that are ‘incorrect’.   
53      It is apparent from Article 6(1)(d) of Directive 95/46 that the assessment of whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected. That purpose consists, as far as the answers submitted by an examination candidate are concerned, in being able to evaluate the level of knowledge and competence of that candidate at the time of the examination. That level is revealed precisely by any errors in those answers. Consequently, such errors do not represent inaccuracy, within the meaning of Directive 95/46, which would give rise to a right of rectification under Article 12(b) of that directive.  
54      On the other hand, it is possible that there might be situations where the answers of an examination candidate and the examiner’s comments with respect to those answers prove to be inaccurate, within the meaning of Article 6(1)(d) of Directive 95/46, for example due to the fact that, by mistake, the examination scripts were mixed up in such a way that the answers of another candidate were ascribed to the candidate concerned, or that some of the cover sheets containing the answers of that candidate are lost, so that those answers are incomplete, or that any comments made by an examiner do not accurately record the examiner’s evaluation of the answers of the candidate concerned.   
55      Moreover, as stated by the Advocate General in point 37 of her Opinion, it cannot be ruled out that a candidate may, under Article 12(b) of Directive 95/46, have the right to ask the data controller to ensure that his examination answers and the examiner’s comments with respect to them are, after a certain period of time, erased, that is to say, destroyed. Pursuant to Article 6(1)(e) of that directive, personal data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is subsequently processed. Taking into consideration the purpose of the answers submitted by an examination candidate and of the examiner’s comments with respect to those answers, their retention in a form permitting the identification of the candidate is, a priori, no longer necessary as soon as the examination procedure is finally closed and can no longer be challenged, so that those answers and comments have lost any probative value.   
56      In so far as the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers are therefore liable to be checked for, in particular, their accuracy and the need for their retention, within the meaning of Article 6(1)(d) and (e) of Directive 95/46, and may be subject to rectification or erasure, under Article 12(b) of the directive, the Court must hold that to give a candidate a right of access to those answers and to those comments, under Article 12(a) of that directive, serves the purpose of that directive of guaranteeing the protection of that candidate’s right to privacy with regard to the processing of data relating to him (see,   
a contrario  
, judgment of 17 July 2014,   
YS and Others  
, C-141/12 and C-372/12, EU:C:2014:2081, paragraphs 45 and 46), irrespective of whether that candidate does or does not also have such a right of access under the national legislation applicable to the examination procedure.  
57      In that context, it must be recalled that the protection of the fundamental right to respect for private life means, inter alia, that any individual may be certain that the personal data relating to him is correct and that it is processed in a lawful manner. As is apparent from recital 41 of Directive 95/46, it is in order to be in a position to carry out the necessary checks that the data subject has, under Article 12(a) of the directive, a right of access to the data relating to him which is being processed. That right of access is necessary, inter alia, to enable the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of his data by the data controller and consequently to exercise the right set out in Article 12(b) of that directive (judgment of 17 July 2014,   
YS and Others  
, C-141/12 and C-372/12, EU:C:2014:2081, paragraph 44 and the case-law cited).  
58      Last, it must be said, first, that the rights of access and rectification, under Article 12(a) and (b) of Directive 95/46, do not extend to the examination questions, which do not as such constitute the candidate’s personal data.  
59      Second, Directive 95/46 and Regulation 2016/679 which replaces the directive both provide for certain restrictions on those rights.   
60      Thus, under Article 13(1)(g) of Directive 95/46, Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in, inter alia, Article 6(1) and Article 12 of that directive, when such a restriction constitutes a necessary measure to safeguard the rights and freedoms of others.  
61      Article 23(1)(e) of Regulation 2016/679 extends the list of grounds justifying restrictions, currently laid down in Article 13(1) of Directive 95/46, to ‘other important objectives of general public interest of the Union or of a Member State’. Further, Article 15(4) of Regulation 2016/679, that article relating to the data subject’s right of access, provides that the right to obtain a copy of personal data must not adversely affect the rights and freedoms of others.  
62      In the light of all the foregoing, the answer to the questions referred is that Article 2(a) of Directive 95/46 must be interpreted as meaning that, in circumstances such as those of the main proceedings, the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data, within the meaning of that provision.  
   
Costs  
63      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that, in circumstances such as those of the main proceedings, the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data, within the meaning of that provision.  
Ilešič  
Rosas  
Toader  
Prechal  
   
Jarašiūnas  
Delivered in open court in Luxembourg on 20 December 2017.  
A. Calot Escobar  
   
M. Ilešič  
Registrar  
   
President of the Second Chamber  
\*      Language of the case: English.  
   
  
  
  
  
Disclaimer

ID: 061e5e93-d725-4de3-9856-f7bb27c6e8b3

Judgment of 17 Jun 2021, C-597/19 (  
M.I.C.M.  
)  
   
JUDGMENT OF THE COURT (Fifth Chamber)  
17 June 2021 (\*)  
(Reference for a preliminary ruling – Intellectual property – Copyright and related rights – Directive 2001/29/EC – Article 3(1) and (2) – Concept of ‘making available to the public’ – Downloading of a file containing a protected work via a peer-to-peer network and the simultaneous provision for uploading pieces of that file – Directive 2004/48/EC – Article 3(2) – Misuse of measures, procedures and remedies – Article 4 – Persons entitled to apply for the application of measures, procedures and remedies – Article 8 – Right of information – Article 13 – Concept of ‘prejudice’ – Regulation (EU) 2016/679 – Point (f) of the first subparagraph of Article 6(1) – Protection of natural persons with regard to the processing of personal data – Lawfulness of processing – Directive 2002/58/EC – Article 15(1) – Legislative measures to restrict the scope of the rights and obligations – Fundamental rights – Articles 7 and 8, Article 17(2) and the first paragraph of Article 47 of the Charter of Fundamental Rights of the European Union)  
In Case C-597/19,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Ondernemingsrechtbank Antwerpen (Companies Court, Antwerp, Belgium), made by decision of 29 July 2019, received at the Court on 6 August 2019, in the proceedings  
Mircom International Content Management & Consulting (M.I.C.M.) Limited  
v  
Telenet BVBA,  
intervening parties:  
Proximus NV,  
Scarlet Belgium NV,  
THE COURT (Fifth Chamber),  
composed of E. Regan, President of the Chamber, M. Ilešič (Rapporteur), E. Juhász, C. Lycourgos and I. Jarukaitis, Judges,  
Advocate General: M. Szpunar,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 10 September 2020,  
after considering the observations submitted on behalf of:  
–        Mircom International Content Management & Consulting (M.I.C.M.) Limited, by T. Toremans and M. Hügel, advocaten,  
–        Telenet BVBA, by H. Haouideg, avocat, and S. Debaene, advocaat,  
–        Proximus NV and Scarlet Belgium NV, by B. Van Asbroeck, avocat, and I. De Moortel and P. Hechtermans, advocaten,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by P. Pucciariello, avvocato dello Stato,  
–        the Austrian Government, by J. Schmoll, acting as Agent,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the European Commission, by F. Wilman and H. Kranenborg and by J. Samnadda, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 17 December 2020,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 3(1) and (2) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10), of Article 3(2), and of Articles 4, 8 and 13 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum OJ 2004 L 195, p. 16), and of point (f) of the first subparagraph of Article 6(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1), read together with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’).  
2        The request has been made in proceedings between Mircom International Content Management Consulting (M.I.C.M.) Limited (‘Mircom’), a company incorporated under Cypriot law, the holder of certain rights over a large number of pornographic films produced by eight undertakings established in the United States and Canada, and Telenet BVBA, a company established in Belgium, providing, inter alia, Internet access services, concerning the latter’s refusal to provide information enabling its customers to be identified on the basis of several thousand IP addresses collected, on behalf of Mircom, by a specialised company, from a peer-to-peer network, where certain Telenet clients, by using the BitTorrent protocol, have allegedly made available films from Mircom’s catalogue.  
   
Legal context  
   
European Union law  
   
Intellectual property law  
–         
Directive 2001/29  
3        Recitals 3, 4, 9, 10, 23 and 31 of Directive 2001/29 are worded as follows:  
‘(3)      The proposed harmonisation will help to implement the four freedoms of the internal market and relates to compliance with the fundamental principles of law and especially of property, including intellectual property, and freedom of expression and the public interest.  
(4)      A harmonised legal framework on copyright and related rights, through increased legal certainty and while providing for a high level of protection of intellectual property, will foster substantial investment in creativity and innovation …  
…  
(9)      Any harmonisation of copyright and related rights must take as a basis a high level of protection, since such rights are crucial to intellectual creation. Their protection helps to ensure the maintenance and development of creativity in the interests of authors, performers, producers, consumers, culture, industry and the public at large. Intellectual property has therefore been recognised as an integral part of property.  
(10)      If authors or performers are to continue their creative and artistic work, they have to receive an appropriate reward for the use of their work, as must producers in order to be able to finance this work. The investment required to produce products such as phonograms, films or multimedia products, and services such as “on-demand” services, is considerable. Adequate legal protection of intellectual property rights is necessary in order to guarantee the availability of such a reward and provide the opportunity for satisfactory returns on this investment.  
…  
(31)      A fair balance of rights and interests between the different categories of right holders, as well as between the different categories of right holders and users of protected subject matter, must be safeguarded. …’  
4        Article 3 of that directive, entitled ‘Right of communication to the public of works and right of making available to the public other subject matter’, provides:  
‘1.      Member States shall provide authors with the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.  
2.      Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:  
…  
(c)      for the producers of the first fixations of films, of the original and copies of their films;  
…  
3.      The rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article.’  
–         
Directive 2004/48  
5        Recitals 10, 14 and 18 of Directive 2004/48 are worded as follows:  
‘(10)      The objective of this Directive is to approximate legislative systems so as to ensure a high, equivalent and homogeneous level of protection in the Internal Market.  
…  
(14)      The measures provided for in Articles 6(2), 8(1) and 9(2) need to be applied only in respect of acts carried out on a commercial scale. This is without prejudice to the possibility for Member States to apply those measures also in respect of other acts. Acts carried out on a commercial scale are those carried out for direct or indirect economic or commercial advantage; this would normally exclude acts carried out by end-consumers acting in good faith.  
…  
(18)      The persons entitled to request application of those measures, procedures and remedies should be not only the rightholders but also persons who have a direct interest and legal standing in so far as permitted by and in accordance with the applicable law, which may include professional organisations in charge of the management of those rights or for the defence of the collective and individual interests for which they are responsible.’  
6        Article 2 of that directive, entitled ‘Scope’, provides, in paragraphs 1 and 3(a):  
‘1.      Without prejudice to the means which are or may be provided for in Community or national legislation, in so far as those means may be more favourable for rightholders, the measures, procedures and remedies provided for by this Directive shall apply, in accordance with Article 3, to any infringement of intellectual property rights as provided for by Community law and/or by the national law of the Member State concerned.  
…  
3.      This Directive shall not affect:  
(a)      the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC [of 24 October 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)] …’  
7        Chapter II of Directive 2004/48, entitled ‘Measures, procedures and remedies’, comprises Articles 3 to 15. Article 3 of that directive, entitled ‘General obligation’, provides:  
‘1.      Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time limits or unwarranted delays.  
2.      Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.’  
8        Under Article 4 of Directive 2004/48, entitled ‘Persons entitled to apply for the application of measures, procedures and remedies’:  
‘Member States shall recognise as persons entitled to seek application of the measures, procedures and remedies referred to in this chapter:  
(a)      the holders of intellectual property rights, in accordance with the provisions of the applicable law,  
(b)      all other persons authorised to use those rights, in particular licensees, in so far as permitted by and in accordance with the provisions of the applicable law,  
(c)      intellectual property collective rights management bodies which are regularly recognised as having a right to represent holders of intellectual property rights, in so far as permitted by and in accordance with the provisions of the applicable law,  
(d)      professional defence bodies which are regularly recognised as having a right to represent holders of intellectual property rights, in so far as permitted by and in accordance with the provisions of the applicable law.’  
9        Article 6(2) of that directive, that article being headed ‘Evidence’, provides:  
‘Under the same conditions, in the case of an infringement committed on a commercial scale Member States shall take such measures as are necessary to enable the competent judicial authorities to order, where appropriate, on application by a party, the communication of banking, financial or commercial documents under the control of the opposing party, subject to the protection of confidential information.’  
10      Article 8 of that directive, entitled ‘Right of information’, provides:  
‘1.      Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:  
(a)      was found in possession of the infringing goods on a commercial scale;  
(b)      was found to be using the infringing services on a commercial scale;  
(c)      was found to be providing on a commercial scale services used in infringing activities; or  
(d)      was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.  
2.      The information referred to in paragraph 1 shall, as appropriate, comprise:  
(a)      the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;  
(b)      information on the quantities produced, manufactured, delivered, received or ordered, as well as the price obtained for the goods or services in question.  
3.      Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which:  
(a)      grant the rightholder rights to receive fuller information;  
(b)      govern the use in civil or criminal proceedings of the information communicated pursuant to this Article;  
(c)      govern responsibility for misuse of the right of information; or  
(d)      afford an opportunity for refusing to provide information which would force the person referred to in paragraph 1 to admit to [his/her] own participation or that of [his/her] close relatives in an infringement of an intellectual property right; or  
(e)      govern the protection of confidentiality of information sources or the processing of personal data.’  
11      In accordance with Article 9(2) of Directive 2004/48, entitled ‘Provisional and precautionary measures’:  
‘In the case of an infringement committed on a commercial scale, the Member States shall ensure that, if the injured party demonstrates circumstances likely to endanger the recovery of damages, the judicial authorities may order the precautionary seizure of the movable and immovable property of the alleged infringer, including the blocking of his bank accounts and other assets. To that end, the competent authorities may order the communication of bank, financial or commercial documents, or appropriate access to the relevant information.’  
12      Under Article 13 of that directive, entitled ‘Damages’:  
‘1.      Member States shall ensure that the competent judicial authorities, on application of the injured party, order the infringer who knowingly, or with reasonable grounds to know, engaged in an infringing activity, to pay the rightholder damages appropriate to the actual prejudice suffered by him as a result of the infringement.  
When the judicial authorities set the damages:  
(a)      they shall take into account all appropriate aspects, such as the negative economic consequences, including lost profits, which the injured party has suffered, any unfair profits made by the infringer and, in appropriate cases, elements other than economic factors, such as the moral prejudice caused to the rightholder by the infringement;  
or  
(b)      as an alternative to (a), they may, in appropriate cases, set the damages as a lump sum on the basis of elements such as at least the amount of royalties or fees which would have been due if the infringer had requested authorisation to use the intellectual property right in question.  
2.      Where the infringer did not knowingly, or with reasonable grounds to know, engage in infringing activity, Member States may lay down that the judicial authorities may order the recovery of profits or the payment of damages, which may be pre-established.’  
–         
Directive 2014/26/EU  
13      Article 39 of Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and the grant of multi-territorial licences for music rights for online use in the internal market (OJ 2014 L 84, p. 72), entitled ‘Notification of collective management organisations’, provides:  
‘By 10 April 2016, Member States shall provide the Commission, on the basis of the information at their disposal, with a list of the collective management organisations established in their territories.  
Member States shall notify any changes to that list to the Commission without undue delay.  
The Commission shall publish that information and keep it up to date.’  
   
Provisions concerning the protection of personal data  
–         
Directive 95/46  
14      In Chapter II, Section II, of Directive 95/46, entitled ‘Criteria for making data processing legitimate’, Article 7(f) of that directive provided:  
‘Member States shall provide that personal data may be processed only if:  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
15      Article 8(1) and (2)(e) of that directive was worded as follows:  
‘1.      Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.  
2.      Paragraph 1 shall not apply where:  
…  
(e)      the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.’  
16      Article 13(1)(g) of that directive provided:  
‘Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:  
…  
(g)      the protection of the data subject or of the rights and freedoms of others.’  
–         
Regulation 2016/679  
17      Article 4 of Regulation 2016/679, entitled ‘Definitions’, states in paragraphs 1, 2, 9 and 10:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(9)      “recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. …’  
(10)      “third party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.’  
18      Article 6 of that regulation, entitled ‘Lawfulness of processing’, provides in point (f) of the first subparagraph of paragraph 1 and the second subparagraph:  
‘Processing shall be lawful only if and to the extent that at least one of the following applies:  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.’  
19      Article 9 of that regulation, entitled ‘Processing of special categories of personal data’, provides, in paragraph 2(e) and (f), that the prohibition on the processing of certain types of personal data revealing in particular data concerning the sexual life or sexual orientation of a natural person does not apply where the processing relates to personal data which are manifestly made public by the data subject or is necessary, in particular, for the establishment, exercise or defence of a right in legal proceedings.  
20      Article 23 of Regulation 2016/679, entitled ‘Restrictions’, provides in paragraph 1(i) and (j):  
‘Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as in Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
…  
(i)      the protection of the data subject or of the rights and freedoms of others;  
(j)      the enforcement of civil law claims.’  
21      Under Article 94 of Regulation 2016/679, entitled ‘Repeal of Directive [95/46]’:  
‘1.      Directive [95/46] is repealed with effect from 25 May 2018.  
2.      References to the repealed Directive shall be construed as references to this Regulation. …’  
22      Article 95 of that regulation, entitled ‘Relationship with Directive [2002/58]’, states:  
‘This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive [2002/58].’  
–         
Directive 2002/58  
23      Article 1 of Directive 2002/58, entitled ‘Scope and aim’, provides in paragraphs 1 and 2:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.  
2.      The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. …’  
24      The second subparagraph of Article 2 of Directive 2002/58, entitled ‘Definitions’, contains the following provision in point (b):  
‘The following definitions shall also apply:  
…  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.’  
25      Article 5 of the directive, entitled ‘Confidentiality of the communications’, provides:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
2.      Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
26      Article 6 of that directive, entitled ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
4.      The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
6.      Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.’  
27      Article 15 of Directive 2002/58, entitled ‘Application of certain provisions of Directive [95/46]’, provides, in paragraph 1 thereof:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’  
   
Belgian law  
28      Under the fourth subparagraph of Article XI.165(1) of the Wetboek Economisch Recht (Code of Economic Law), the author of a literary or artistic work alone has the right to communicate it to the public by any means, including by making available to the public in such a way that members of the public may access them from a place and at a time individually chosen by them.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
29      On 6 June 2019, Mircom brought an action before the Ondernemingsrechtbank Antwerpen (Companies Court, Antwerp, Belgium) seeking, inter alia, that Telenet be ordered to produce the identification data for its customers whose Internet connections had been used to share, on a peer-to-peer network by means of the BitTorrent protocol, films from the Mircom catalogue.  
30      Mircom claims to have thousands of dynamic IP addresses recorded on its behalf, thanks to the FileWatchBT software, by Media Protector GmbH, a company established in Germany, at the time of the connection of those Telenet customers using the Bit-Torrent client sharing software.  
31      Telenet, supported by two other Internet access providers established in Belgium, Proximus NV and Scarlet Belgium NV, oppose Mircom’s action.  
32      In the first place, in the light of the judgment of 14 June 2017,   
Stichting Brein  
 (C-610/15, EU:C:2017:456), which concerned communication to the public, within the meaning of Article 3(1) of Directive 2001/29, by the operators of an Internet sharing platform in the context of a peer-to-peer network, the referring court asks whether such a communication to the public may be made by individual users of such a network, called ‘downloaders’, who, by downloading pieces of a digital file containing a copyrighted work, simultaneously make those pieces available for uploading by other users. Those users, belonging to a group of persons who download, called the ‘swarm’, thus themselves become ‘seeders’ of those pieces, like the undetermined initial seeder, who is at the origin of the first provision of that file in that network.  
33      In that regard, the referring court states, first, that the pieces are not mere fragments of the original file, but autonomous encrypted files which are unusable in themselves, and, second, that, because of the way in which BitTorrent technology functions, the uploading of the pieces of a file, known as ‘seeding’, is, in principle, automatic, as that characteristic can be eliminated only by certain programs.  
34      However, Mircom claims that even downloads of pieces representing together a proportion of at least 20% of the underlying media file should be taken into account, since, on the basis of that percentage, it becomes possible to obtain an overview of that file, although fragmentary and of highly uncertain quality.  
35      In the second place, the referring court doubts whether an undertaking, such as Mircom, can enjoy the protection conferred by Directive 2004/48, in so far as it does not actually use the rights assigned by the authors of the films at issue, but merely claims damages from alleged infringers, a model which resembles the definition of a ‘copyright troll’.  
36      In the third place, the question also arises as to the lawfulness of the manner in which the IP addresses were collected by Mircom, in the light of point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679.  
37      It was in those circumstances that the Ondernemingsrechtbank Antwerpen (Companies Court, Antwerp) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      (a)      Can the downloading of a file via a peer-to-peer network and the simultaneous provision for uploading of parts thereof … (which may be very fragmentary as compared to the whole) (‘seeding’) be regarded as a communication to the public within the meaning of Article 3(1) of Directive 2001/29, even if the individual pieces as such are unusable?  
If so,  
(b)      is there a   
de minimis  
 threshold above which the seeding of those pieces would constitute a communication to the public?  
(c)      is the fact that seeding can take place automatically (as a result of the BitTorrent client settings), and thus without the user’s knowledge, relevant?  
(2)      (a)      Can a person who is the contractual holder of the copyright (or related rights), but does not himself exploit those rights and merely claims damages from alleged infringers – and whose economic business model thus depends on the existence of piracy, not on combating it – enjoy the same rights as those conferred by Chapter II of Directive 2004/48 on authors or licence holders who exploit copyright in the normal way?  
(b)      How can the licence holder in that case have suffered “prejudice” (within the meaning of Article 13 of Directive 2004/48) as a result of the infringement?  
(3)      Are the specific circumstances set out in Questions 1 and 2 relevant when assessing the correct balance to be struck between, on the one hand, the enforcement of intellectual property rights and, on the other, the rights and freedoms safeguarded by the [Charter of Fundamental Rights of the European Union], such as respect for private life and protection of personal data, in particular in the context of the assessment of proportionality?  
(4)      Is, in all those circumstances, the systematic registration and general further processing of the IP-addresses of a “swarm” of “seeders” (by the licence holder himself or herself, and by a third party on his or her behalf) legitimate under Regulation [2016/679], and specifically under Article 6(1) [first subparagraph] (f) thereof?’  
   
Consideration of the questions referred  
   
The first question  
38      It should be noted as a preliminary point that, in the procedure laid down by Article 267 TFEU providing for cooperation between national courts and the Court of Justice, it is for the latter to provide the national court with an answer which will be of use to it and enable it to determine the case before it. To that end, the Court may have to reformulate the questions referred to it. The Court has a duty to interpret all provisions of EU law which national courts require in order to decide on the actions pending before them, even if those provisions are not expressly indicated in the questions referred to the Court by those courts (judgment of 19 December 2019,   
Nederlands Uitgeversverbond and Groep Algemene Uitgevers  
, C-263/18, EU:C:2019:1111, paragraph 31 and the case-law cited).  
39      To that end, the Court can extract from all the information provided by the national court, in particular from the grounds of the order for reference, the points of EU law which require interpretation in view of the subject matter of the dispute in the main proceedings (judgment of 19 December 2019,   
Nederlands Uitgeversverbond and Groep Algemene Uitgevers  
, C-263/18, EU:C:2019:1111, paragraph 32 and the case-law cited).  
40      In the present case, by its first question, the referring court asks the Court, in essence, whether the concept of ‘communication to the public’, referred to in Article 3(1) of Directive 2001/29, covers the sharing, on a peer-to-peer network, of sometimes very fragmentary pieces of a media file containing a protected work. However, as the Advocate General observed in point 34 of his Opinion, in so far as, in the main proceedings, the rights of film producers are concerned, it appears that, in the present case, it is rather Article 3(2)(c) of that directive which could apply.  
41      In that context, since the EU legislature did not express a different intention, the expression ‘making available to the public’, used in Article 3(1) of Directive 2001/29 as a form of authors’ exclusive right to authorise or prohibit any ‘communication to the public’, and the identical expression in Article 3(2) of that directive, designating an exclusive right belonging to the holders of related rights, must be interpreted as having the same meaning (see, by analogy, judgment of 2 April 2020,   
Stim and SAMI  
, C-753/18, EU:C:2020:268, paragraph 28 and the case-law cited).  
42      In the light of those considerations, it is necessary to reformulate the first question to the effect that, by that question, the referring court asks, in essence, whether Article 3(1) and (2) of Directive 2001/29 must be interpreted as meaning that the uploading, from the terminal equipment of a user of a peer-to-peer network to such equipment of other users of that network, of pieces, previously downloaded by that user, of a media file containing a protected work, although those pieces are usable in themselves only as from a certain download rate and that, because of the configurations of the BitTorrent client sharing software, that uploading is automatically generated by that software, constitutes making available to the public, within the meaning of that provision.  
43      First of all, it must be noted that, as the Advocate General observed in point 48 of his Opinion, those pieces are not parts of works, but parts of the files containing those works, used for transmitting those files under the BitTorrent protocol. Accordingly, the fact that the pieces which are transmitted are unusable in themselves is irrelevant since what is made available is the file containing the work, that is to say the work in digital format.  
44      In that regard, as the Advocate General observed in point 49 of his Opinion, the operation of peer-to-peer peer networks does not differ, in essence, from the operation of the Internet in general or, more specifically, from the World Wide Web, where the files containing a work are divided into small data packages, which are routed between the server and the client in a random order and by different channels.  
45      In the present case, as is apparent from the order for reference, any user of the peer-to-peer network can easily reconstruct the original file from pieces available on the computers of users participating in the same swarm. The fact that a user does not succeed, individually, in downloading the entire original file does not prevent him or her from making available to his or her peers the pieces of that file which he or she has managed to download onto his or her computer and that he or she thus contributes to the creation of a situation in which, ultimately, all the users participating in the swarm have access to the complete file.  
46      In order to establish that there is ‘making available’ within the meaning of Article 3(1) and (2) of Directive 2001/29 in such a situation, it is not necessary to prove that the user concerned has previously downloaded a number of pieces representing a minimum threshold.  
47      In order for there to be an ‘act of communication’, and consequently, an act of making available, it is sufficient, in the final analysis, that a work is made available to a public in such a way that the persons comprising that public may access it, from wherever and whenever they individually choose, irrespective of whether or not they avail themselves of that opportunity (see, to that effect, judgment of 7 August 2018,   
Renckhoff  
, C-161/17, EU:C:2018:634, paragraph 20). The concept of an ‘act of communication’ refers, in that regard, to any transmission of the protected works, irrespective of the technical means or process used (judgment of 29 November 2017,   
VCAST  
, C-265/16, EU:C:2017:913; paragraph 42 and the case-law cited).  
48      Therefore, any act whereby a user, in full knowledge of the consequences of what he or she is doing, gives access to protected work is liable to constitute an act of communication for the purposes of Article 3(1) and (2) of Directive 2001/29 (see, to that effect, judgment of 9 March 2021,   
VG Bild-Kunst  
, C-392/19, EU:C:2021:181, paragraph 30 and the case-law cited).  
49      In the present case, it appears that any user of the peer-to-peer network at issue, who has not deactivated the upload function of the BitTorrent client sharing software, uploads onto that network the pieces of media files that he or she has previously downloaded onto his or her computer. Provided that it is apparent, which it is for the referring court to determine, that the relevant users of that network have subscribed to that software by giving their consent to its application after having been duly informed of its characteristics, those users must be regarded as acting in full knowledge of their conduct and of the consequences which it may have. Once it is established that they have actively subscribed to such software, the deliberate nature of their conduct is in no way negated by the fact that the uploading is automatically generated by that software.  
50      If it follows from the foregoing considerations that, subject to factual verification which it is for the referring court to carry out, the conduct of the users concerned is capable of constituting an act of making available a work or other protected subject matter, it is then necessary to examine whether such conduct constitutes making available to ‘the public’ within the meaning of Article 3(1) and (2) of Directive 2001/29.  
51      In that regard, it must be recalled that, in order to come within the concept of ‘making available to the public’, within the meaning of that provision, works or other subject matter must in fact be made available to a public, that making available referring to an indeterminate number of potential recipients and involving a fairly large number of persons. Moreover, that making available to the public must be communicated using specific technical means, different from those previously used or, failing that, to a new public, that is to say, to a public that was not already taken into account by the rightholder of any copyright or related right when he or she authorised the initial communication of his or her work or of other protected subject matter to the public (see, to that effect, judgment of 9 March 2021,   
VG Bild-Kunst  
, C-392/19, EU:C:2021:181, paragraphs 31 and 32 and the case-law cited).  
52      As regards peer-to-peer networks, the Court has already held that the making available and management, on the Internet, of a sharing platform which, by means of indexation of metadata referring to protected works and the provision of a search engine, allows users of that platform to locate those works and to share them in the context of such a network constitutes a communication to the public within the meaning of Article 3(1) of Directive 2001/29 (judgment of 14 June 2017,   
Stichting Brein  
, C-610/15, EU:C:2017:456, paragraph 48).  
53      In the present case, as the Advocate General found, in essence, in points 37 and 61 of his Opinion, the computers of those users sharing the same file constitute the peer-to-peer network itself, called the ‘swarm’, in which they play the same role as the servers in the operation of the World Wide Web.  
54      It is common ground that such a network is used by a considerable number of persons, as is apparent, moreover, from the high number of IP addresses registered by Mircom. Moreover, those users can access, at any time and simultaneously, the protected works which are shared by means of the platform.  
55      Consequently, that making available is aimed at an indeterminate number of potential recipients and involves a fairly large number of persons.  
56      Furthermore, in so far as the case concerns works published without the authorisation of the rightholders, it must also be considered that those works are made available to a new public (see, by analogy, judgment of 14 June 2017,   
Stichting Brein  
, C-610/15, EU:C:2017:456, paragraph 45 and the case-law cited).  
57      In any event, even if it were found that a work has been previously posted on a website, without any restriction preventing it from being downloaded and with the consent of the rightholder of any copyright or related rights, the fact that, through a peer-to-peer network, users such as those at issue in the main proceedings have downloaded parts of the file containing that work on a private server, followed by those pieces being made available by means of uploading those pieces into the same network, means that those users have played a decisive role in making that work available to a public which was not taken into account by the rightholder of any copyright or related rights in that work when he or she authorised the initial communication (see, by analogy, judgment of 7 August 2018,   
Renckhoff  
, C-161/17, EU:C:2018:634, paragraphs 46 and 47).  
58      If such making available, by uploading a work, without the rightholder of the copyright or related rights over it being able to rely on the rights laid down in Article 3(1) and (2) of Directive 2001/29, constitutes it being made available, the consequence would be that the need to safeguard a fair balance, referred to in recitals 3 and 31 of that directive, in the digital environment between, on one hand, the interest of the holders of copyright and related rights in the protection of their intellectual property, guaranteed in Article 17(2) of the Charter of Fundamental Rights (‘the Charter’) and, on the other hand, the protection of the interests and fundamental rights of users of protected subject matter, in particular their freedom of expression and information guaranteed in Article 11 of the Charter, as well as the public interest, would be disregarded (see, to that effect, judgment of 9 March 2021,   
VG Bild-Kunst  
, C-392/19, EU:C:2021:181, paragraph 54 and the case-law cited). Disregard of that balance would, moreover, undermine the principal objective of Directive 2001/29, which, as is apparent from recitals 4, 9 and 10 thereof, is to establish a high level of protection for rightholders, enabling rightholders to obtain an appropriate reward for the use of their protected works or other subject matter, in particular when they are made available to the public.  
59      In the light of the foregoing considerations, the answer to the first question is that Article 3(1) and (2) of Directive 2001/29 must be interpreted as meaning that the uploading, from the terminal equipment of a user of a peer-to-peer network to such equipment of other users of that network, of pieces, previously downloaded by that user, of a media file containing a protected work, even though those pieces are usable in themselves only as from a certain download rate, constitutes making available to the public within the meaning of that provision. It is irrelevant that, due to the configurations of the BitTorrent client sharing software, that uploading is automatically generated by it, when the user, from whose terminal equipment that uploading takes place, has subscribed to that software by giving his or her consent to its application after having been duly informed of its characteristics.  
   
The second question  
60      By its second question, the referring court asks, in essence, whether Directive 2004/48 must be interpreted as meaning that a person who is the contractual holder of certain intellectual property rights, who does not however use them himself or herself, but merely claims damages from alleged infringers, may benefit from the measures, procedures and remedies provided for in Chapter II of that directive.  
61      That question must be understood as covering three parts, namely, first, that relating to the legal standing of a person such as Mircom to seek the application of the measures, procedures and remedies provided for in Chapter II of Directive 2004/48, secondly, the question whether such a person may have suffered prejudice within the meaning of Article 13 of that directive and, thirdly, the question concerning the admissibility of his or her request for information, pursuant to Article 8 of that directive, read in conjunction with Article 3(2) thereof.  
62      As regards the first part, relating to Mircom’s legal standing to bring proceedings, it must be borne in mind that the person seeking the application of the measures, procedures and remedies provided for in Chapter II of Directive 2004/48 must fall within one of the four categories of persons or bodies listed in Article 4(a) to (d) thereof.  
63      Those categories include, first, holders of intellectual property rights, secondly, all the other persons authorised to use those rights, in particular licensees, thirdly, intellectual property collective rights management bodies which are regularly recognised as having a right to represent holders of intellectual property rights, and, fourth, professional defence bodies which are regularly recognised as having a right to represent holders of intellectual property rights.  
64      However, unlike the holders of intellectual property rights referred to in Article 4(a) of Directive 2004/48, in accordance with recital 18 of that directive, the three categories of persons referred to in Article 4(b) to (d) thereof must also have a direct interest in the defence of those rights and the right to be a party to legal proceedings in so far as permitted by, and in accordance with, the applicable legislation (see, to that effect, judgment of 7 August 2018,   
SNB-REACT  
, C-521/17, EU:C:2018:639, paragraph 39).  
65      In the present case, the possibility that Mircom may be a collective management body or a professional defence body within the meaning of Article 4(c) and (d) of Directive 2004/48 should be ruled out from the outset. As the Advocate General observed in points 92 and 93 of his Opinion, Mircom does not, as it itself states, have the task of managing the copyright and related rights of its contractual parties or of ensuring the professional defence of the latter, but seeks solely to obtain compensation for prejudice resulting from infringements of those rights.  
66      In that context, it should be noted that the activities of those bodies are harmonised within the Union by Directive 2014/26. Mircom’s name does not appear on the list of collective management bodies published by the European Commission in accordance with Article 39 of that directive.  
67      As regards the status of holder of intellectual property rights, within the meaning of Article 4(a) of Directive 2004/48, in so far as that provision does not require such a rightholder to actually use his or her intellectual property rights, that right cannot be excluded from the scope of that provision on account of the non-use of those rights.  
68      In that regard, it should be noted that the referring court classifies Mircom as a person who is contractually the holder of copyright or related rights. In those circumstances, Mircom should be granted the benefit of the measures, procedures and remedies provided for by Directive 2004/48 notwithstanding the fact that it does not use those rights.  
69      A company such as Mircom could, moreover, be considered, in any event, to be another person authorised to use intellectual property rights within the meaning of Article 4(b) of that directive, it being understood that that authorisation also does not presuppose an actual use of the assigned rights. The fact of being classified as an ‘other person’, within the meaning of Article 4(b) of that directive, must, however, as noted in paragraph 64 above, be verified in accordance with the provisions of the applicable legislation, that reference having to be understood, in the light of Article 2(1) of that directive, as referring both to the relevant national legislation and, as the case may be, to EU legislation (see, to that effect, judgment of 7 August 2018,   
SNB-REACT  
, C-521/17, EU:C:2018:639, paragraph 31).  
70      As regards the second part of the second question, it concerns, in particular, the fact that, in the present case, Mircom does not use and does not appear to have any intention of using the rights acquired over the works at issue in the main proceedings. According to the referring court, that non-use of the assigned rights casts doubt on the possibility of such a person suffering prejudice within the meaning of Article 13 of Directive 2004/48.  
71      That question concerns the actual identity of the injured party who has suffered, here, prejudice, within the meaning of Article 13 of that directive, as a result of the infringement of intellectual property rights, namely whether the prejudice at issue was suffered by Mircom or by the producers of the films concerned.  
72      It is true that holders of intellectual property rights, referred to in Article 4(a) of Directive 2004/48, and the persons authorised to use those rights, referred to in Article 4(b) of that directive, may be harmed, in principle, by infringing activities, in so far as, as the Advocate General noted, in essence, in point 70 of his Opinion, those activities may hinder the normal use of those rights or diminish their revenue. However, it is also possible that a person, while having intellectual property rights, may merely recover, in his or her own name and on his or her own behalf, damages in respect of claims assigned to him or her by other holders of intellectual property rights.  
73      In the present case, the referring court appears to take the view that Mircom merely acts, before it, as assignee, providing the film producers at issue with a service for the collection of claims for damages.  
74      It must be held that the fact that a person referred to in Article 4 of Directive 2004/48 merely brings such an action as assignee is not such as to exclude him or her from the benefit of the measures, procedures and remedies provided for in Chapter II of that directive.  
75      Such an exclusion runs counter to the general objective of Directive 2004/48, which is, as is clear from recital 10 thereof, to ensure a high level of protection of intellectual property in the internal market (see, to that effect, judgment of 18 January 2017,   
NEW WAVE CZ  
, C-427/15, EU:C:2017:18, paragraph 23).  
76      It should be noted, in that regard, that an assignment of claims cannot, in itself, affect the nature of the rights which have been infringed, in the present case, the intellectual property rights of the film producers concerned, in particular in the sense that that assignment has an effect on the determination of the court having jurisdiction or on other procedural aspects, such as the possibility of seeking measures, procedures and remedies, within the meaning of Chapter II of Directive 2004/48 (see, by analogy, judgment of 21 May 2015,   
CDC Hydrogen Peroxide  
, C-352/13, EU:C:2015:335, paragraphs 35 and 36 and the case-law cited).  
77      Consequently, if a holder of intellectual property rights chose to outsource the recovery of damages to a specialised undertaking by assigning claims or another legal act, he or she should not suffer less favourable treatment than another owner of such rights who would choose to assert those rights personally. Such treatment would undermine the attractiveness of that outsourcing from an economic point of view and would ultimately deprive holders of intellectual property rights of that possibility, which is moreover widespread in various fields of law, such as that of protection of air passengers, provided for in Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 (OJ 2004 L 46, p. 1).  
78      As regards the third part of its second question, the referring court harbours doubts, in essence, as to the admissibility of Mircom’s request for information, made under Article 8 of Directive 2004/48, in so far as that company does not make serious use of the rights which it has acquired from the film producers at issue in the main proceedings. Furthermore, it must be understood that, by referring to the possibility of classifying Mircom as a ‘copyright troll’, the referring court raises, in essence, the question of the existence of a possible abuse of rights by Mircom.  
79      In the first place, the referring court appears to be doubtful as to whether Mircom intended to bring an action for damages, in so far as there is strong evidence that, generally, it merely proposes an amicable settlement with the sole aim of obtaining a lump sum of damages of EUR 500. In accordance with Article 8(1) of Directive 2004/48, a request for information must be made in the context of proceedings relating to an infringement of an intellectual property right.  
80      As noted by the Advocate General in point 113 of his Opinion, it must be held, in that regard, that seeking an amicable solution is often a prerequisite for bringing an action for damages in the strict sense. Consequently, it cannot be considered that, in the context of the system for the protection of intellectual property established by Directive 2004/48, that practice is prohibited.  
81      The Court has already held that Article 8(1) of Directive 2004/48 must be interpreted as applying to a situation in which, after the definitive termination of proceedings in which it was held that an intellectual property right was infringed, an applicant in separate proceedings seeks information on the origin and distribution networks of the goods or services by which that intellectual property right is infringed (judgment of 18 January 2017,   
NEW WAVE CZ  
, C-427/15, EU:C:2017:18, paragraph 28).  
82      It is appropriate to apply the same reasoning in relation to a separate procedure preceding an action for damages, such as that at issue in the main proceedings, in which, under Article 8(1)(c) of Directive 2004/48, an applicant requests an Internet service provider, such as Telenet, which has been found to be providing, on a commercial scale, services used in infringing activities, the information enabling its customers to be identified with a view, specifically, to being able usefully to bring legal proceedings against the alleged infringers.  
83      The right to information, provided for in Article 8 of the Charter, seeks to apply and implement the fundamental right to an effective remedy guaranteed in Article 47 of the Charter, and thereby to ensure the effective exercise of the fundamental right to property, which includes the intellectual property right protected in Article 17(2) of the Charter by enabling the holder of an intellectual property right to identify the person who is infringing that right and take the necessary steps in order to protect it (judgment of 9 July 2020,   
Constantin Film Verleih  
, C-264/19, EU:C:2020:542, paragraph 35).  
84      Consequently, it must be held that a request for information such as that made by Mircom during a pre-litigation stage cannot, for that reason alone, be regarded as inadmissible.  
85      In the second place, according to Article 8(1) of Directive 2004/48, such a request must be justified and proportionate.  
86      It must be stated, in the light of the considerations set out in paragraphs 70 to 77 above, that that may be the case where the request referred to in Article 8(1), is submitted by a company which is contractually authorised in that regard by film producers. It is, however, for the referring court to determine whether the request, as specifically formulated by such a company, is well founded.  
87      In the third place, referring to the expression ‘any unfair profits made by the infringer’, used in point (a) of the second subparagraph of Article 13(1) of Directive 2004/48, and to the condition laid down in Article 6(2), Article 8(1) and Article 9(2) thereof, that infringements must be carried out on a commercial scale, the referring court considers that the EU legislature had in mind here the situation requiring structural action against the spread of counterfeiting on the market, and not the fight against individual infringers.  
88      In that regard, it should be noted, first, that, in accordance with recital 14 of Directive 2004/48, the condition that infringements must be carried out on a commercial scale need to be applied only to measures relating to the evidence provided for in Article 6 of that directive, to the measures concerning the right to information provided for in Article 8 thereof and to the provisional and protective measures provided for in Article 9 of that directive, without prejudice to the possibility for Member States also to apply those measures to acts which are not carried out on a commercial scale.  
89      That condition does not apply to the injured party’s claims for damages against an infringer referred to in Article 13 of Directive 2004/48. Consequently, under that provision, individual infringers may be ordered to pay the owner of the intellectual property rights damages appropriate to the actual prejudice suffered by him as a result of the infringement, provided that the infringer knowingly or with reasonable grounds to know engaged in the infringing activity.  
90      Furthermore, in the context of a request for information under Article 8(1) of Directive 2004/48, the condition that the infringements must be committed in a commercial context may be satisfied in particular where a person other than the alleged infringer ‘was found to be providing on a commercial scale services used in infringing activities’.  
91      In the present case, Mircom’s request for information is, as stated in paragraph 82 of the present judgment, directed against an Internet service provider, as a person found in the process of providing, on a commercial scale, services used in infringing activities.  
92      Consequently, in the dispute in the main proceedings, Mircom’s request against Telenet, which provides, on a commercial scale, services used in infringing activities, appears to satisfy the condition referred to in paragraph 90 of the present judgment.  
93      Furthermore, it is for the referring court to ascertain, in any event, whether Mircom has abused measures, procedures and remedies within the meaning of Article 3 of Directive 2004/48 and, if necessary, to refuse that company’s request.  
94      Article 3 of Directive 2004/48 imposes a general obligation to ensure, inter alia, that the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by that directive, including the right of information referred to in Article 8, are fair and equitable and applied in such a way as to provide for safeguards against their abuse.  
95      The possible finding of such abuse falls entirely within the scope of the assessment of the facts in the main proceedings and, therefore, within the jurisdiction of the referring court. That court could in particular, to that end, examine Mircom’s operating method, by evaluating the way in which Mircom offers amicable solutions to alleged infringers and by ascertaining whether it actually brings legal proceedings in the event of a refusal to reach an amicable solution. It could also examine whether, in the light of all the particular circumstances of the present case, Mircom is in fact attempting, under the guise of proposing amicable solutions to alleged infringements, to extract economic revenue from the very membership of the users concerned in a peer-to-peer network such as the one at issue, without specifically seeking to combat the copyright infringements caused by that network.  
96      In the light of the foregoing considerations, the answer to the second question is that Directive 2004/48 must be interpreted as meaning that a person who is the contractual holder of certain intellectual property rights, who does not however use them himself or herself, but merely claims damages from alleged infringers, may benefit, in principle, from the measures, procedures and remedies provided for in Chapter II of that directive, unless it is established, in accordance with the general obligation laid down in Article 3(2) of that directive and on the basis of an overall and detailed assessment, that his or her request is abusive. In particular, as regards a request for information based on Article 8 of that directive, it must also be rejected if it is unjustified or disproportionate, which is for the referring court to determine.  
   
The third and fourth questions  
97      As a preliminary point, it should be noted that, in the case in the main proceedings, there are two different types of personal data processing at issue, namely one which has already been carried out, upstream, by Media Protector and on behalf of Mircom, in the context of peer-to-peer networks, consisting of the recording of the IP addresses of users whose Internet connections were allegedly used, at a given time, for the uploading of protected works on those networks, and the other, which, according to Mircom, must be carried out downstream by Telenet, consisting, first, of the identification of those users by means of a match between those IP addresses and those which, at the same time, Telenet had allocated to those users for the purpose of carrying out that uploading and, second, of the communication to Mircom of the names and addresses of the same users.  
98      In its fourth question, the referring court seeks an answer as to whether, in the light of point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679, only the first processing which has already been carried out is justified.  
99      Furthermore, in its third question, it seeks to ascertain, in essence, whether the circumstances set out in its first and second questions are relevant for the purposes of assessing the fair balance between, on the one hand, the right to intellectual property and, on the other hand, the protection of privacy and personal data, in particular in the assessment of proportionality.  
100    In the event that, on the basis of the Court’s answers to the first and second questions, the referring court finds that Mircom’s request for information satisfies the conditions laid down in Article 8 of Directive 2004/48, read in conjunction with Article 3(2) thereof, it must be understood that, by its third question, the referring court seeks to ascertain, in essence, whether, in circumstances such as those at issue in the main proceedings, point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679 must be interpreted as precluding the second downstream processing, as described in paragraph 97 of the present judgment, even though that request satisfies those conditions.  
101    In the light of those considerations and in accordance with the case-law cited in paragraphs 38 and 39 of the present judgment, it is necessary to reformulate the third and fourth questions to the effect that, by those questions, the referring court asks, in essence, whether point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679 must be interpreted as precluding, first, the systematic registration, by the holder of intellectual property rights and by a third party acting on that holder’s behalf, of the IP addresses of users of peer-to-peer networks whose Internet connections have allegedly been used in infringing activities and, second, the communication of the names and of postal addresses of those users to the rightholder or to a third party in order to enable him or her to bring a claim for damages before a civil court for prejudice allegedly caused by those users.  
102    In the first place, as regards the upstream processing at issue in the main proceedings, it must be recalled that a dynamic IP address registered by an online media services provider when a person accesses a website which that provider makes accessible to the public constitutes personal data, within the meaning of Article 4(1) of Regulation 2016/679, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the Internet service provider has about that person (judgment of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 49).  
103    Consequently, the registration of such addresses for the purposes of their subsequent use in legal proceedings constitutes processing within the meaning of Article 4(2) of Regulation 2016/679.  
104    That is also the situation of Mircom, on behalf of whom Media Protector collects the IP addresses, in so far as it has a legal means of identifying the owners of the Internet connections in accordance with the procedure provided for in Article 8 of Directive 2004/48.  
105    Under point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679, the processing of personal data is lawful only if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
106    Accordingly, that provision lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or freedoms and fundamental rights of the person concerned by the data protection do not take precedence (see, to that effect, as regards Article 7(f) of Directive 95/46, judgment of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 28).  
107    Since Regulation 2016/679 repealed and replaced Directive 95/46 and the relevant provisions of that regulation have essentially the same scope as that of the relevant provisions of that directive, the Court’s case-law on that directive is also applicable, in principle, to that regulation (see, by analogy, judgment of 12 November 2020,   
Sonaecom  
, C-42/19, EU:C:2020:913, paragraph 29).  
108    As regards the condition relating to the pursuit of a legitimate interest and subject to verifications which it is for the referring court to carry out in the context of the second question, it must be held that the interest of the controller or of a third party in obtaining the personal information of a person who allegedly damaged their property in order to sue that person for damages can be qualified as a legitimate interest. That analysis is supported by Article 9(2)(e) and (f) of Regulation 2016/679, which provides that the prohibition on the processing of certain types of personal data, such as that revealing the sex life or sexual orientation of a natural person, is not to apply, in particular, where the processing concerns personal data which is clearly rendered public by the person concerned or is necessary for the establishment, exercise or defence of legal claims (see, to that effect, as regards Article 8(2)(e) of Directive 95/46, judgment of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 29).  
109    In that regard, as the Advocate General stated, in essence, in point 131 of his Opinion, the recovery of claims in the prescribed manner by an assignee may constitute a legitimate interest justifying the processing of personal data in accordance with point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679 (see, by analogy, as regards Directive 2002/58, judgment of 22 November 2012,   
Probst  
, C-119/12, EU:C:2012:748, paragraph 19).  
110    As regards the condition relating to the necessity of processing personal data for the purposes of the legitimate interests pursued, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (judgment of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 30). That condition could, in the present case, be satisfied since, as the Advocate General observed in point 97 of his Opinion, identification of the owner of the connection is often possible only on the basis of the IP address and the information provided by the Internet service provider.  
111    Finally, as regards the condition of balancing of the opposing rights and interests at issue, it depends in principle on the specific circumstances of the particular case (judgment of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 31 and the case-law cited). It is for the referring court to assess those particular circumstances.  
112    In that regard, the mechanisms allowing the different rights and interests to be balanced are contained in Regulation 2016/679 itself (see, by analogy, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 66 and the case-law cited).  
113    Moreover, in so far as the facts in the main proceedings seem to fall within both the scope of Regulation 2016/679 and that of Directive 2002/58, the IP addresses processed constitute, as is clear from the case-law cited in paragraph 102 of the present judgment both personal data and traffic data (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 152), it must be ascertained whether the assessment of the lawfulness of such processing must take account of the conditions laid down by that directive.  
114    As is apparent from Article 1(2) of Directive 2002/58, read in conjunction with Article 94(2) of Regulation 2016/679, the provisions of that directive specify and supplement that regulation in order to harmonise the national provisions necessary to ensure, in particular, an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, as regards the processing of personal data in the electronic communications sector (see, to that effect, judgments of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 31, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 102).  
115    In that regard, it should be noted that, under Article 5(1) of Directive 2002/58, Member States are to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1) of that directive. Furthermore, under Article 6(1) of that directive, traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice, in particular, to Article 15(1) of that directive.  
116    Article 15(1) ends the list of exceptions to the obligation to ensure the confidentiality of personal data with an express reference to Article 13(1) of Directive 95/46, corresponding, in essence, to Article 23(1) of Regulation 2016/679, which now allows both EU law and the law of the Member State to which the controller or processor is subject to restrict, by means of legislative measures, the scope of the obligation of confidentiality of personal data in the electronic communications sector, where that restriction respects the essence of the freedoms and the fundamental freedoms and that it constitutes a necessary and proportionate measure in a democratic society to ensure, in particular, the protection of the rights and freedoms of others and the enforcement of civil law claims (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 53).  
117    Furthermore, the fact that Article 23(1)(j) of that regulation now expressly refers to the enforcement of claims under civil law must be interpreted as expressing the intention of the EU legislature to confirm the case-law of the Court according to which the protection of the right to property and situations in which authors seek to obtain such protection in civil proceedings have never been excluded from the scope of Article 15(1) of Directive 2002/58 (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 53).  
118    Consequently, in order for processing, such as the registration of IP addresses of persons whose Internet connections have been used to upload pieces of files containing protected works on peer-to-peer networks, for the purposes of filing a request for disclosure of the names and postal addresses of the holders of those IP addresses, can be regarded as lawful by satisfying the conditions laid down by Regulation 2016/679, it is necessary, in particular, to ascertain whether that processing satisfies the abovementioned provisions of Directive 2002/58, which embodies, for users of electronic communications, the fundamental rights to respect for private life and the protection of personal data (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 109).  
119    In the absence in the order for reference of details relating to the legal basis for Mircom’s access to the IP addresses retained by Telenet, the Court is not in a position to provide the referring court with useful guidance as to whether processing such as that carried out upstream, consisting of the registration of those IP addresses, undermines those fundamental rights, in the light of the rules set out in Directive 2002/58 and the condition relating to the balancing of conflicting rights and interests. It will be for the referring court to analyse the relevant national legislation in the light of EU law, in particular Articles 5, 6 and 15 of Directive 2002/58.  
120    In the second place, as regards Telenet’s downstream processing, which consists of identifying the holders of those IP addresses and communicating to Mircom the names and postal addresses of those holders, it should be noted that a request, in accordance with Article 8 of Directive 2004/48, limited to the disclosure of the names and addresses of users involved in infringing activities is consistent with the objective of striking a fair balance between the rights of intellectual property rightholders and the right of users to protection of personal data (see, to that effect, judgment of 9 July 2020,   
Constantin Film Verleih  
, C-264/19, EU:C:2020:542, paragraphs 37 and 38 and the case-law cited).  
121    Such data relating to the civil identity of users of electronic communications systems do not normally, in themselves, make it possible to ascertain the date, time, duration and recipients of the communications made, or the locations where those communications took place or their frequency with specific people during a given period, with the result that they do not provide, apart from the contact details of those users, such as their civil status, addresses, any information on the communications sent and, consequently, on the users’ private lives. Thus, the interference entailed by a measure relating to those data cannot, in principle, be classified as serious (see, to that effect, judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 34 and the case-law cited).  
122    That said, in the case in the main proceedings, Mircom’s request for information presupposes that Telenet performs a match between the dynamic IP addresses recorded on behalf of Mircom and those allocated by Telenet to those users, who have allowed them to participate in the peer-to-peer network at issue.  
123    Consequently, as is apparent from the case-law cited in paragraph 113 of the present judgment, such a request concerns the processing of traffic data. The right to protection of that data, which is enjoyed by the persons referred to in Article 8(1) of Directive 2004/48, forms part of the fundamental right of every person to have his or her personal data protected, as guaranteed by Article 8 of the Charter and Regulation 2016/679, as clarified and supplemented by Directive 2002/58 (see, to that effect, judgment of 16 July 2015,   
Coty Germany  
, C-580/13, EU:C:2015:485, paragraph 30).  
124    The application of the measures provided for by Directive 2004/48 cannot, in fact, affect Regulation 2016/679 and Directive 2002/58 (see, to that effect, judgment of 16 July 2015,   
Coty Germany  
, C-580/13, EU:C:2015:485, paragraph 32).  
125    In that regard, the Court has already held that Article 8(3) of Directive 2004/48, read in conjunction with Article 15(1) of Directive 2002/58 and Article 7(f) of Directive 95/46, does not preclude Member States from imposing an obligation to disclose to private persons personal data in order to enable them to bring civil proceedings for copyright infringements, but nor does it require those Member States to lay down such an obligation (see, to that effect, judgments of 19 April 2012,   
Bonnier Audio and Others  
, C-461/10, EU:C:2012:219, paragraph 55 and the case-law cited, and of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 34).  
126    It should be noted that, like Article 7(f) of Directive 95/46, neither point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679 nor Article 9(2)(f) of that regulation, although directly applicable in any Member State, by virtue of the second paragraph of Article 288 TFEU, imposes an obligation on a third party, such as an Internet service provider, to communicate to private persons, as recipients, within the meaning of Article 4(9) of that regulation, personal data for the purpose of prosecuting copyright infringements before the civil courts, but merely regulate the issue of the lawfulness of the processing by the controller itself or by a third party, within the meaning of Article 4(10) of that regulation.  
127    Thus, an Internet service provider such as Telenet could be obliged to make such a communication only on the basis of a measure, referred to in Article 15(1) of Directive 2002/58, which limits the scope of the rights and obligations laid down, inter alia, in Articles 5 and 6 thereof.  
128    In so far as the order for reference contains no information in that regard, the referring court will have to ascertain the legal basis both of Telenet’s retention of the IP addresses of which Mircom requests disclosure and of any access to those addresses by Mircom.  
129    In accordance with Article 6(1) and (2) of Directive 2002/58, the retention of IP addresses by providers of electronic communications services beyond the period for which that data is assigned does not, in principle, appear to be necessary for the purpose of billing the services at issue, with the result that the detection of offences committed online may therefore prove impossible without recourse to a legislative measure under Article 15(1) of Directive 2002/58 (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 154).  
130    As the Advocate General observed, in essence, in point 104 of his Opinion, if the retention of IP addresses on the basis of such a legislative measure or, at the very least, their use for purposes other than those considered to be lawful in the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), were to be regarded as contrary to EU law, the request for information in the main proceedings would become devoid of purpose.  
131    If it were to follow from the investigations carried out by the referring court that there are national legislative measures, within the meaning of Article 15(1) of Directive 2002/58, which limit the scope of the rules laid down in Articles 5 and 6 of that directive and which could usefully apply to the present case, and on the assumption that it is also apparent, on the basis of the interpretative guidance provided by the Court in all of the preceding paragraphs of the present judgment, that Mircom has legal standing to bring proceedings and that its request for information is justified, proportionate and not abusive, the abovementioned processing must be regarded as lawful, within the meaning of Regulation 2016/679.  
132    In the light of the foregoing considerations, the answer to the third and fourth questions is that point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679, read in conjunction with Article 15(1) of Directive 2002/58, must be interpreted as meaning that it precludes in principle, neither the systematic recording, by the holder of intellectual property rights as well as by a third party on his or her behalf, of IP addresses of users of peer-to-peer networks whose Internet connections have allegedly been used in infringing activities, nor the communication of the names and of the postal addresses of those users to that rightholder or to a third party in order to enable it to bring claim for damages before a civil court for prejudice allegedly caused by those users, provided, however, that the initiatives and the requests to that effect by that rightholder or such a third party are justified, proportionate and not abusive and have their legal basis in a national legislative measure, within the meaning of Article 15(1) of Directive 2002/58, which limits the scope of the rules laid down in Articles 5 and 6 of that directive.  
   
Costs  
133    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Fifth Chamber) hereby rules:  
1.        
Article 3(1) and (2) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the uploading, from the terminal equipment of a user of a peer-to-peer network to such equipment of other users of that network, of pieces, previously downloaded by that user, of a media file containing a protected work, even though those pieces are usable in themselves only as from a certain download rate, constitutes making available to the public within the meaning of that provision. It is irrelevant that, due to the configurations of the BitTorrent client sharing software, that uploading is automatically generated by it, when the user, from whose terminal equipment that uploading takes place, has subscribed to that software by giving his or her consent to its application after having been duly informed of its characteristics.  
2.        
Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights must be interpreted as meaning that a person who is the contractual holder of certain intellectual property rights, who does not however use them himself or herself, but merely claims damages for alleged infringers, may benefit, in principle, from the measures, procedures and remedies provided for in Chapter II of that directive, unless it is established, in accordance with the general obligation laid down in Article 3(2) of that directive and on the basis of an overall and detailed assessment, that his or her request is abusive. In particular, as regards a request for information based on Article 8 of that directive, it must also be rejected if it is unjustified or disproportionate, which is for the referring court to determine.  
3.        
Point (f) of subparagraph 1 of Article 6(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), read in conjunction with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, must be interpreted as meaning that it precludes in principle, neither the systematic recording, by the holder of intellectual property rights as well as by a third party on his or her behalf, of IP addresses of users of peer-to-peer networks whose Internet connections have allegedly been used in infringing activities, nor the communication of the names and of the postal addresses of those users to that rightholder or to a third party in order to enable it to bring a claim for damages before a civil court for prejudice allegedly caused by those users, provided, however, that the initiatives and requests to that effect of that rightholder or of such a third party are justified, proportionate and not abusive and have their legal basis in a national legislative measure, within the meaning of Article 15(1) of Directive 2002/58, which limits the scope of the rules laid down in Articles 5 and 6 of that directive, as amended.

ID: 0724d257-a065-4010-adc1-f5895d224e9d

of 11 Dec 2019, C-708/18 (  
Asociatia de Proprietari bloc M5A-ScaraA  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
   
JUDGMENT OF THE COURT (Third Chamber)  
11 December 2019 (\*)  
[Text rectified by order of 13 February 2020]   
(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Charter of Fundamental Rights of the European Union — Articles 7 and 8 — Directive 95/46/EC — Article 6(1)(c) and Article 7(f) — Making the processing of personal data legitimate — National legislation allowing video surveillance for the purposes of ensuring the safety and protection of individuals, property and valuables and for the pursuit of legitimate interests, without the data subject’s consent — Installation of a video surveillance system in the common parts of a residential building)  
In Case C-708/18,  
REQUEST for a preliminary ruling under Article 267 TFEU from Tribunalul Bucureşti (Regional Court, Bucharest, Romania), made by decision of 2 October 2018, received at the Court on 6 November 2018, in the proceedings  
TK  
v  
Asociaţia de Proprietari bloc M5A-ScaraA,  
THE COURT (Third Chamber),  
composed of A. Prechal (Rapporteur), President of the Chamber, L.S. Rossi, J. Malenovský, F. Biltgen and N. Wahl, Judges,  
Advocate General: G. Pitruzzella,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        the Romanian Government, by C.-R. Canţăr, O.-C. Ichim and A. Wellman, acting as Agents,  
–        the Czech Government, by M. Smolek, J. Vláčil and O. Serdula, acting as Agents,  
–        the Danish Government, by J. Nymann-Lindegren, M. Wolff and P.Z.L. Ngo, acting as Agents,  
–        [As rectified by order of 13 February 2020] Ireland, by M. Browne, G. Hodge and A. Joyce, acting as Agents, and by D. Fennelly, Barrister-at-Law,  
–        the Austrian Government, initially by G. Hesse and J. Schmoll, and subsequently by J. Schmoll, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes, P. Barros da Costa, L. Medeiros, I. Oliveira and M. Cancela Carvalho, acting as Agents,  
–        the European Commission, by H. Kranenborg, D. Nardi and L. Nicolae, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 6(1)(e) and Article 7(f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), and of Articles 8 and 52 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between TK and the Asociaţia de Proprietari bloc M5A-ScaraA (Association of co-owners of building M5A, staircase A, ‘the association of co-owners’) concerning TK’s application for an order that the association take out of operation the building’s video surveillance system and remove the cameras installed in the common parts of the building.  
   
Legal context  
   
EU  
 law  
3        Directive 95/46 was repealed and replaced, with effect from 25 May 2018, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (OJ 2016 L 119, p. 1). However, given the date of the facts at issue in the main proceedings, those proceedings remain governed by Directive 95/46.  
4        According to Article 1 thereof, Directive 95/46 seeks to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and to remove the obstacles to flows of those data.  
5        Article 3(1) of that directive provided:  
‘This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.’  
6        Chapter II of that directive included Section I, entitled ‘Principles relating to Data Quality’, comprising Article 6 of the directive, which provided:  
‘1.      Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.  
2.      It shall be for the controller to ensure that paragraph 1 is complied with’.  
7        In Section II of Chapter II, entitled ‘Criteria for Making Data Processing Legitimate’, Article 7 of Directive 95/46 was worded as follows:  
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent;  
or  
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;  
or  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
or  
(d)      processing is necessary in order to protect the vital interests of the data subject;  
or  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;  
or  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
   
Romanian law  
8        Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Law No 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) (  
Monitorul Oficial  
, Part I, No 790 of 12 December 2001), as amended by Law No 102/2005 and Government Emergency Order No 36/2007, applicable   
ratione temporis   
 to the main proceedings, was adopted in order to transpose Directive 95/46 into Romanian law.  
9        Article 5 of Law No 667/2001 as amended provided:  
‘1.      Any personal data processing, except for the processing which refers to the categories mentioned in Article 7(1) and Articles 8 and 10, may be carried out only if the data subject has given his or her express and unequivocal consent for that processing.  
2.      The data subject’s consent is not required in the following situations:  
(a)      when the processing is required in order to carry out a contract or an agreement previous to that contract to which the data subject is a party, or in order to adopt measures, at his or her request, before the signing of the contract or previous agreement;  
(b)      when the processing is required in order to protect the data subject’s life, physical integrity or health or those of a threatened third party;  
(c)      when the processing is required in order to fulfil a legal obligation of the data controller;  
(d)      when the processing is required in order to accomplish a measure of public interest or concerning the exercise of public powers of the data controller or the third party to whom the data are disclosed;  
(e)      when the processing is necessary in order to accomplish a legitimate interest of the data controller or of the third party to whom the data are disclosed, on the condition that that interest does not adversely affect the interests or the fundamental rights and freedoms of the data subject;  
(f)      when the processing concerns data which is obtained from publicly accessible documents, according to the law;  
(g)      when the processing is performed exclusively for statistical purposes, historical or scientific research and the data remain anonymous throughout the entire processing.  
3.      The provisions of paragraph 2 are without prejudice to the legal texts governing the obligations of public authorities to respect and protect personal, family and private life.’  
10      Decision No 52/2012 of the Autoritate Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (the National Authority for the Supervision of the Processing of Personal Data, Romania, ‘the ANSPDCP’) concerning the processing of personal data through the use of video surveillance systems, in the version applicable to the main proceedings, provided, in Article 1 thereof:  
‘The collection, recording, storage, use, transmission, disclosure or any other operation for the processing of images by video surveillance means, which enable individuals to be identified directly or indirectly, constitute the processing of personal data falling within the scope of [Law No 677/2001].’  
11      Article 4 of that decision provided:  
‘Video surveillance may primarily be carried out for the following purposes:  
(a)      the prevention and countering of crime;  
(b)      road-traffic surveillance and the detection of road-traffic offences;  
(c)      the safety and protection of persons, property and assets, and buildings and public facilities and their enclosures;  
(d)      the implementation of public-interest measures or the exercise of public powers;  
(e)      the pursuit of legitimate interests, provided that the rights and fundamental freedoms of data subjects are not adversely affected.’  
12      Article 5(1) to (3) of that decision states:  
‘1.      Video surveillance may be carried out in open or public places and spaces, including on public-access roadways located on public or private land, subject to the conditions provided for by law.  
2.      Video surveillance cameras shall be installed so that they are visible.  
3.      The use of concealed video surveillance shall be prohibited, except in the cases provided for by law.’  
13      Article 6 of that decision stated:  
‘The processing of personal data using video surveillance means shall be carried out with the express and unequivocal consent of the data subject or in the cases referred to in Article 5(2) of Law No 677/2001 ….’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
14      TK lives in an apartment which he owns, located in the building M5A. At the request of certain co-owners of that building, the association of co-owners adopted, at a general assembly held on 7 April 2016, a decision approving the installation of video surveillance cameras in that building.  
15      In implementation of that decision, three video surveillance cameras were installed in the common parts of the M5A building. The first camera was pointed towards the front of the building, whereas the second and third cameras were installed, respectively, in the ground-floor hallway and in the building’s lift.  
16      TK objected to that video surveillance system being installed, on the ground that it constituted an infringement of the right to respect for private life.  
17      Having found that, notwithstanding the numerous steps undertaken by him and the written acknowledgment of the association of co-owners that the video surveillance system installed was unlawful, that system continued to operate, TK brought an action before the referring court requesting that the association of co-owners be ordered to remove the three cameras and to take them out of operation definitively, failing which a penalty payment would be imposed.  
18      TK argued before the referring court that the video surveillance system at issue infringed EU primary and secondary law, in particular the right to respect for private life both under EU and national law. He also stated that the association of co-owners had taken on the task of data controller for personal data without having followed the registration procedure in that regard provided for by law.  
19      The association of co-owners stated that the decision to install a video surveillance system had been taken in order to monitor as effectively as possible who enters and leaves the building, since the lift had been vandalised on many occasions and there had been burglaries and thefts in several apartments and the common parts.  
20      The association also stated that other measures which it had taken previously, namely the installation of an intercom/magnetic card entry system, had not prevented repeat offences of the same nature being committed.  
21      In addition, the association of co-owners sent TK the memorandum which it had drawn up with the company which had installed the video surveillance cameras, stating that on 21 October 2016 the system’s hard drive had been erased and disconnected, that it had been taken out of operation and that the images recorded had been deleted.  
22      The association also communicated to TK another memorandum, dated 18 May 2017 from which it is apparent that the three video surveillance cameras had been uninstalled. That memorandum stated that the association of co-owners had, in the meantime, completed the procedure enabling it to be registered as data controller responsible for personal data.  
23      TK stated, however, before the referring court that the three video surveillance cameras were still in place.  
24      The referring court notes that Article 5 of Law No 677/2001 provides, in a general manner, that processing of personal data, such as the recording of images by means of a video surveillance system, may be carried out only if the data subject has given his or her express and unequivocal consent. Paragraph 2 of that article sets out, however, a series of exceptions to that rule, which include the exception whereby the processing of personal data is required in order to protect the data subject’s life, physical integrity or health or those of a threatened third party. Decision No 52/2012 of the ANSPDCP provides for the same type of exception.  
25      The referring court makes reference, next, to Article 52(1) of the Charter enshrining the principle that there must be proportionality between the aim pursued by the interference with the rights and freedoms of citizens and the means used.  
26      According to that court, the video surveillance system at issue before it does not seem to have been used in a manner or for a purpose not corresponding to the stated objective of the association of co-owners, which is that of protecting the life, physical integrity or health of the data subjects, namely the co-owners of the building in which that system was installed.  
27      In those circumstances Tribunalul Bucureşti (Regional Court, Bucharest, Romania) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Are Articles 8 and 52 of the Charter and Article 7(f) of Directive 95/46 to be interpreted as precluding provisions of national law such as those at issue in the main proceedings, namely Article 5(2) of [Law No 677/2001], and Article 6 of [Decision No 52/2012 of the ANSPDCP], in accordance with which video surveillance may be used to ensure the safety and protection of individuals, property and valuables and for the pursuit of legitimate interests, without the data subject’s consent?  
(2)      Are Articles 8 and 52 of the Charter to be interpreted as meaning that the limitation of rights and freedoms which results from video surveillance is in accordance with the principle of proportionality, satisfies the requirement of being ‘necessary’ and ‘meets objectives of general interest or the need to protect the rights and freedoms of others’, where the controller is able to take other measures to protect the legitimate interest in question?  
(3)      Is Article 7(f) of Directive 95/46 to be interpreted as meaning that the ‘legitimate interests’ of the controller must be proven, present and effective at the time of the data processing?  
(4)      Is Article 6(1)(e) of Directive 95/46 to be interpreted as meaning that data processing (video surveillance) is excessive or inappropriate where the controller is able to take other measures to protect the legitimate interest in question?’  
   
Consideration of the questions referred  
28      First of all, it must be found that although the referring court does, by its fourth question, refer to Article 6(1)(e) of Directive 95/46, it provides no explanation as to the relevance of that provision to the outcome of the dispute in the main proceedings.  
29      Article 6(1)(e) relates only to the requirements governing the storage of personal data. Nothing in the documents before the Court permits the inference that the dispute in the main proceedings concerns that aspect.  
30      By contrast, in so far as by that question the referring court asks, in essence, whether the installation of a video surveillance system, such as that at issue before it, is proportionate to the purposes pursued, it must be found that the issue of whether personal data collected by that system meet the requirement of proportionality relates to the interpretation of Article 6(1)(c) of Directive 95/46.  
31      Article 6(1)(c) of Directive 95/46 must be taken into account when verifying the second condition of application laid down in Article 7(f) of Directive 95/46, according to which the processing of personal data is ‘necessary’ for the purposes of the legitimate interests pursued.  
32      Secondly, by its first and second questions, Tribunalul Bucureşti (Regional Court, Bucharest, Romania) refers to Articles 8 and 52 of the Charter, taken in isolation or read in conjunction with Article 7(f) of Directive 95/46. The Court has made clear that the assessment of the condition laid down in that provision, relating to the existence of fundamental rights and freedoms of the data subject which override the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the particular case in question, and in the context of which account must be taken of the significance of the data subject’s rights arising from Articles 7 and 8 of the Charter (judgment of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 40). It follows that Articles 8 and 52 of the Charter must not, in the present case, be applied in isolation.  
33      In the light of the foregoing, it must be found that, by its questions, which must be examined together, the referring court asks, in essence, whether Article 6(1)(c) and Article 7(f) of Directive 95/46, read in the light of Articles 7 and 8 of the Charter, must be interpreted as precluding national provisions which authorise the installation of a system of video surveillance, such as the system at issue in the main proceedings, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the data subject’s consent.  
34      It must be borne in mind that surveillance in the form of a video recording of persons, which is stored on a continuous recording device — the hard disk drive — constitutes, pursuant to Article 3(1) of Directive 95/46, the automatic processing of personal data (judgment of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraph 25).  
35      Consequently, a video surveillance system using a camera must be characterised as the automatic processing of personal data, within the meaning of that provision, where the device installed enables personal data, such as images allowing natural persons to be identified, to be recorded and stored. It is for the referring court to ascertain whether the system at issue in the main proceedings has such characteristics.  
36      In addition, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of Directive 95/46 and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of that directive (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 71 and the case-law cited).  
37      Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of the cases in which the processing of personal data can be regarded as being lawful. The Member States cannot add new principles relating to the lawfulness of the processing of personal data in that article or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article (judgment of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 57).  
38      It follows that, in order to be considered lawful, the processing of personal data must come within one of the six cases provided for in Article 7 of Directive 95/46.  
39      The questions raised by the referring court concern, in particular, the principle relating to making data processing legitimate referred to in Article 7(f) of Directive 95/46; that provision was transposed into Romanian law by Article 5(2)(e) of Law No 677/2001, and that article is also referred to in Article 6 of Decision No 52/2012 of the ANSPDCP as regards specifically the processing of personal data by video surveillance means.  
40      In that regard, Article 7(f) of Directive 95/46 lays down three cumulative conditions in order for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; secondly, the need to process personal data for the purposes of the legitimate interests pursued; and thirdly, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued (judgment of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 28).  
41      It must be stated that Article 7(f) of Directive 95/46 does not require the data subject’s consent. Such consent, as a condition to which the processing of personal data is made subject, appears, however, only in Article 7(a) of that directive.  
42      In the present case, the objective which the controller essentially seeks to achieve when he or she installs a video surveillance system such as that at issue in the main proceedings, namely protecting the property, health and life of the co-owners of a building, is likely to be characterised as a ‘legitimate interest’, within the meaning of Article 7(f) of Directive 95/46. The first condition laid down in that provision appears, therefore, in principle, to be fulfilled (see, by analogy, judgment of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraph 34).  
43      The referring court is, however, uncertain whether the first of the conditions laid down in Article 7(f) must be understood as meaning that the interests pursued by the controller at issue must, first, be ‘proven’ and, secondly be ‘present and effective at the time of the data processing’.  
44      In that regard, it must be found that, as the Romanian and Czech Governments, Ireland, the Austrian Government, the Portuguese Government and the Commission have argued, since, in accordance with Article 7(f) of Directive 95/46, the controller responsible for the processing of personal data or the third party to whom those data are disclosed must pursue legitimate interests justifying that processing, those interests must be present and effective as at the date of the data processing and must not be hypothetical at that date. It cannot, however, be necessarily required, at the time of examining all the circumstances of the case, that the safety of property and individuals was previously compromised.  
45      In the present case, in a situation such as that at issue in the main proceedings, the condition relating to the existence of a present and effective interest seems in any event to be fulfilled, since the referring court notes that thefts, burglaries and acts of vandalism had occurred before the video surveillance system was installed and that was despite the previous installation, in the entrance to the building, of a security system comprising an intercom/magnetic card entry.  
46      As regards the second condition laid down in Article 7(f) of Directive 95/46, relating to the need to process personal data for the purposes of the legitimate interests pursued, the Court has pointed out that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (judgment of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 30 and the case-law cited).  
47      That condition requires the referring court to ascertain that the legitimate data processing interests pursued by the video surveillance at issue in the main proceedings — which consist, in essence, in ensuring the security of property and individuals and preventing crime — cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.  
48      In addition, as the Commission maintained, the condition relating to the need for processing must be examined in conjunction with the ‘data minimisation’ principle enshrined in Article 6(1)(c) of Directive 95/46, in accordance with which personal data must be ‘adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed’.  
49      It is apparent from the documents before the Court that the requirements linked to the proportionality of the processing of data at issue in the main proceedings seem to have been taken into account. It is not in dispute that alternative measures consisting in a security system, installed in the entrance to the building, and comprising an intercom/magnetic card entry, were initially put in place, but proved to be insufficient. In addition, the video surveillance device at issue is limited only to the common parts of the building in co-ownership and the approach to it.  
50      However, the proportionality of the data processing by a video surveillance device must be assessed by taking into account the specific methods of installing and operating that device, which must limit the effect thereof on the rights and freedoms of data subjects while ensuring the effectiveness of the video surveillance system at issue.  
51      Consequently, as the Commission contended, the condition relating to the need for processing implies that the controller must examine, for example, whether it is sufficient that the video surveillance operates only at night or outside normal working hours, and block or obscure the images taken in areas where surveillance is unnecessary.  
52      Lastly, as regards the third condition laid down in Article 7(f) of Directive 95/46, relating to the existence of fundamental rights and freedoms of the data subject whose data require protection, which might override the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, it must be borne in mind, as mentioned in paragraph 32 above, that the assessment of that condition necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the particular case in question, and in the context of which account must be taken of the significance of the data subject’s rights arising from Articles 7 and 8 of the Charter.  
53      In that context, the Court has held that Article 7(f) of Directive 95/46 precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case. Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case (judgment of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 62).  
54      It is also apparent from the case-law of the Court that it is possible to take into consideration, for the purposes of that balancing, the fact that the seriousness of the infringement of the data subject’s fundamental rights resulting from that processing can vary depending on the possibility of accessing the data at issue in public sources (see, to that effect, judgment of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 32).  
55      Unlike the processing of data from public sources, the processing of data from non-public sources implies that information relating to the data subject’s private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed. This more serious infringement of the data subject’s rights enshrined in Articles 7 and 8 of the Charter must be taken into account and be balanced against the legitimate interest pursued by the data controller or by the third party or parties to whom the data are disclosed (see, to that effect, judgment of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 45).  
56      The criterion relating to the seriousness of the infringement of the data subject’s rights and freedoms is an essential component of the weighing or balancing exercise on a case-by-case basis, required by Article 7(f) of Directive 95/46.  
57      In this respect, account must be taken, inter alia, of the nature of the personal data at issue, in particular of the potentially sensitive nature of those data, and of the nature and specific methods of processing the data at issue, in particular of the number of persons having access to those data and the methods of accessing them.  
58      The data subject’s reasonable expectations that his or her personal data will not be processed when, in the circumstance of the case, that person cannot reasonably expect further processing of those data, are also relevant for the purposes of the balancing exercise.  
59      Lastly, those factors must be balanced against the importance, for all the co-owners of the building concerned, of the legitimate interests pursued in the instant case by the video surveillance system at issue, inasmuch as it seeks essentially to ensure that the property, health and life of those co-owners are protected.  
60      In the light of the foregoing, the answer to the questions raised is that Article 6(1)(c) and Article 7(f) of Directive 95/46, read in the light of Articles 7 and 8 of the Charter, must be interpreted as not precluding national provisions which authorise the installation of a video surveillance system, such as the system at issue in the main proceedings, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the consent of the data subjects, if the processing of personal data carried out by means of the video surveillance system at issue fulfils the conditions laid down in Article 7(f), which it is for the referring court to determine.  
   
Costs  
61      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Article 6(1)(c) and Article 7(f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as not precluding national provisions which authorise the installation of a video surveillance system, such as the system at issue in the main proceedings, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the consent of the data subjects, if the processing of personal data carried out by means of the video surveillance system at issue fulfils the conditions laid down in Article 7(f), which it is for the referring court to determine.

ID: 088d0766-b193-4501-a454-a632525c4e3f

Judgment of 17 Jul 2014, C-141/12 (  
YS and Others  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Processing   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
   
JUDGMENT OF THE COURT (Third Chamber)  
17 July 2014 (\*)  
(Request for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Articles 2, 12 and 13 — Concept of ‘personal data’ — Scope of the right of access of a data subject — Data relating to the applicant for a residence permit and legal analysis contained in an administrative document preparatory to the decision — Charter of Fundamental Rights of the European Union — Articles 8 and 41)  
In Joined Cases C-141/12 and C-372/12,  
REQUESTS for a preliminary ruling under Article 267 TFEU from the Rechtbank Middelburg (C-141/12) and from the Raad van State (C-372/12) (Netherlands), made by decisions of 15 March 2012 and 1 August 2012 respectively, received at the Court on 20 March 2012 and 3 August 2012, in the proceedings  
YS  
 (C-141/12)  
v  
Minister voor Immigratie, Integratie en Asiel,  
and  
Minister voor Immigratie, Integratie en Asiel   
(C-372/12)  
v  
M,  
S,  
THE COURT (Third Chamber),  
composed of M. Ilešič (Rapporteur), President of the Chamber, C.G. Fernlund, A. Ó Caoimh, C. Toader and E. Jarašiūnas, Judges,  
Advocate General: E. Sharpston,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 3 July 2013,  
after considering the observations submitted on behalf of:  
–        YS, M and S, by B. Scholten, J. Hoftijzer and I. Oomen, advocaten,  
–        the Netherlands Government, by B. Koopman and C. Wissels, acting as Agents,  
–        the Czech Government, by M. Smolek, acting as Agent,  
–        the Greek Government, by E.-M. Mamouna and D. Tsagkaraki, acting as Agents,  
–        the French Government, by D. Colas and S. Menez, acting as Agents,  
–        the Austrian Government, by C. Pesendorfer, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,  
–        the European Commission, by B. Martenczuk, P. van Nuffel and C. ten Dam, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 12 December 2013,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern the interpretation of Articles 2(a), 12(a) and 13(1)(d), (f) and (g) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), and of Articles 8(2) and 41(2)(b) of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The requests have been made in two sets of proceedings between YS, a third country national who applied for a residence permit for a fixed period in the Netherlands, and the Minister voor Immigratie, Integratie en Asiel (Minister for Immigration, Integration and Asylum, ‘the Minister’) and between the Minister and M and S, also third country nationals who made the same type of application, concerning the Minister’s refusal to communicate to those nationals a copy of an administrative document drafted before the adoption of the decisions on their applications for residence permits.  
   
Legal context  
   
EU law  
3        Directive 95/46, the object of which, according to Article 1, is to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, and to remove obstacles to the free flow of personal data, states in recitals 25 and 41 in its preamble:  
‘(25)      Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons ... responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;  
...  
(41)      Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; ...’  
4        The concept of ‘personal data’ is defined in Article 2(a) of Directive 95/46 as ‘any information relating to an identified or identifiable natural person (“data subject”)’.  
5        Article 12 of that directive, entitled ‘Right of access’, provides as follows:   
‘Member States shall guarantee every data subject the right to obtain from the controller:  
(a)      without constraint at reasonable intervals and without excessive delay or expense:  
–        confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,  
–        communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,  
...  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
(c)      notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.’  
6        Article 13(1) of that directive, entitled ‘Exemptions and restrictions’, provides:  
‘Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in [Article] ... 12 ... when such a restriction constitutes a necessary [measure] to safeguard:  
…  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
…  
(f)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);  
(g)      the protection of the data subject or of the rights and freedoms of others.’  
7        Article 14 of the directive provides that Member States are to grant the data subject the right, in certain circumstances, to object to the processing of data relating to him.  
8        Under Articles 22 and 23(1) of the directive, Member States are to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question and to provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the directive is entitled to receive compensation from the controller for the damage suffered.  
   
Netherlands law  
9        Articles 2, 12 and 13 of Directive 95/46 were transposed into national law by Articles 1, 35 and 43 respectively of the Law on the Protection of Personal Data (Wet bescherming persoonsgegevens, ‘the Wbp’).  
10      Article 35 of the Wbp is worded as follows:  
‘The data subject shall have the right to apply to the controller without restraint and at reasonable intervals to be notified as to whether data relating to him are being processed. The controller shall notify the data subject in writing within four weeks if data relating to him are being processed.  
Where such data are being processed, such notification shall contain a full overview thereof in an intelligible form, a description of the purpose or purposes of the processing, the categories of data concerned and the recipients or categories of recipients, as well as any available information as to the source of the data.’  
11      Under Article 43(e) of the Wbp, the controller can exclude application of Article 35 of the Wbp in so far as is necessary in the interests of protecting the data subject or the rights and freedoms of others.  
12      Under Article 29(1)(a) of the Law on Foreign Nationals 2000 (Vreemdelingenwet 2000, the ‘Vw 2000’), a residence permit for a fixed period may be granted to a foreign national who is a refugee. Under Article 29(1)(b) of that law, such a permit may also be granted to a foreign national who has proved that he has good grounds for believing that if he is expelled he will run a real risk of being subjected to the death penalty or execution, to torture, inhuman or degrading treatment or punishment, or to serious and individual threat to a civilian’s life or person by reason of indiscriminate violence in situations of international or internal armed conflict.  
   
The disputes in the main proceedings and the questions referred for a preliminary ruling  
13      The case officer of the Immigration and Naturalisation Service responsible for dealing with an application for a residence permit draws up, where he is not authorised to sign the decision, a draft decision which is submitted for assessment to a reviser in that service. The case officer attaches a document in which he explains to the reviser the reasons for his draft decision (‘the minute’). Where the case officer has the authority to sign, the minute is not submitted to a reviser but is used as an explanatory memorandum of the decision making process to justify the decision internally. The minute is part of the preparatory process within that service but not of the final decision, even though some points mentioned in it may reappear in the statement of reasons of that decision.  
14      Generally, the minute contains the following information: name, telephone and office number of the case officer responsible for preparing the decision; boxes for the initials and names of revisers; data relating to the applicant, such as name, date of birth, nationality, gender, ethnicity, religion and language; details of the procedural history; details of the statements made by the applicant and the documents submitted; the legal provisions which are applicable; and, finally, an assessment of the foregoing information in the light of the applicable legal provisions. This assessment is referred to as the ‘legal analysis’.  
15      Depending on the case, the legal analysis may be more or less extensive, varying from a few sentences to several pages. In an in-depth analysis, the case officer responsible for the preparation of the decision addresses, inter alia, the credibility of the statements made and explains why he considers an applicant eligible or not for a residence permit. A summary analysis may merely refer to the application of a particular policy line.  
16      Until 14 July 2009, the Minister’s policy was to make the minute available upon mere request. Taking the view that the large number of those requests resulted in too great a work load, that the data subjects often misinterpreted the legal analyses contained in the minutes which were made available to them and that, because of that availability, the exchange of views within the Immigration and Naturalisation Service was recorded less frequently in the minutes, the Minister abandoned that policy.  
17      Since then, requests for the communication of minutes have been systematically refused. Instead of obtaining a copy of the minute, the applicant now receives a summary of the personal data contained in the document, including information relating to the origin of those data and, where relevant, the bodies to which they were disclosed.  
   
Case C-141/12  
18      On 13 January 2009, YS submitted an application for a residence permit for a fixed period under asylum law. The application was rejected by decision of 9 June 2009. That decision was withdrawn by letter of 9 April 2010, and the application was once again rejected by decision of 6 July 2010.  
19      By letter of 10 September 2010, YS asked for the minute relating to the decision of 6 July 2010 to be communicated to him.  
20      By decision of 24 September 2010, that was refused. However, the decision did give a summary of the data contained in the minute, the origin of those data and the bodies to which the data had been disclosed. YS lodged an objection against the refusal to communicate the minute, which itself was rejected by decision of 22 March 2011.  
21      YS then brought an action against that rejection decision before the Rechtbank Middelburg (District Court, Middelburg), on the ground that he could not lawfully be refused access to that minute.  
22      In those circumstances, the Rechtbank Middelburg decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘1.      Are the data reproduced in the minute concerning the data subject and which relate to the data subject personal data within the meaning of Article 2(a) of [Directive 95/46]?  
2.      Does the legal analysis included in the minute constitute personal data within the meaning of the aforementioned provision?   
3.      If the Court of Justice confirms that the data described above are personal data, should the processor/government body grant access to those personal data pursuant to Article 12 of [Directive 95/46] and Article 8(2) of the Charter?   
4.      In that context, may the data subject rely directly on Article 41(2)(b) of the Charter, and if so, must the phrase “while respecting the legitimate interests of confidentiality [in decision-making]” included therein be interpreted in such a way that the right of access to the minute may be refused on that ground?   
5.      When the data subject requests access to the minute, should the processor/government body provide a copy of that document in order to do justice to the right of access?’  
   
Case C-372/12  
 The dispute concerning M  
23      By decision of 28 October 2009, the Minister granted M a residence permit for a fixed period as asylum seeker on the basis of Article 29(1)(b) of the Vw 2000. The reasons for that decision were not given, in that it did not set out the manner in which the case had been assessed by the Immigration and Naturalisation Service.  
24      By letter of 30 October 2009, M, on the basis of Article 35 of the Wbp, requested access to the minute relating to that decision.  
25      By decision of 4 November 2009, the Minister refused M access to the minute. He based the refusal on Article 43(e) of the Wbp, since he was of the view that access to such a document was liable adversely to affect the freedom of the case worker responsible for compiling it to include certain arguments and considerations in the minute which could be relevant in the decision-making process.  
26      The objection to that refusal having been rejected by decision of 3 December 2010, M brought an action against that decision before the Rechtbank Middelburg. By decision of 16 June 2011, that court took the view that the interest relied on by the Minister to refuse access to the minute did not amount to an interest protected by Article 43(e) of the Wbp, and annulled the Minister’s decision as being based on reasoning that was wrong in law. It also found that there was no reason to maintain the legal effects of the decision, since the Minister, contrary to Article 35(2) of the Wbp, had not given access to the legal analysis in the minute from which it might have become evident why M could not be considered to be a refugee for the purposes of Article 29(1)(a) of the Vw 2000.  
 The dispute concerning S  
27      By decision of 10 February 2010, which did not state reasons, the Minister granted S an ordinary residence permit for a fixed period on the ground of ‘dramatic circumstances’. By letter of 19 February 2010, S, on the basis of Article 35 of the Wbp, requested the minute relating to that decision.  
28      The request was rejected by decision of 31 March 2010, which was confirmed by decision of 21 October 2010 following an objection. In the decision of 21 October 2010, the Minister took the position that the decision of 31 March 2010 had already stated which personal data were included in the minute and that the request for access to the minute had thus been met. Furthermore, he was of the opinion that the Wbp does not confer any rights of access to the minute.  
29      By decision of 4 August 2011, the Rechtbank Amsterdam (District Court, Amsterdam) declared well-founded the action brought by S against the decision of 21 October 2010 and annulled that decision. That court found, inter alia, that the minute in question did not contain any information other than personal data of S, that he had a right of access to those data under the Wbp, and that the Minister’s refusal to allow access was not validly based.  
30      The Minister decided to appeal to the Raad van State (Council of State) both in the dispute concerning M and in that concerning S.  
31      In those circumstances, the Raad van State decided to join the cases concerning M and S, to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘1.       Should the second indent of Article 12(a) of [Directive 95/46] be interpreted to mean that there is a right to a copy of documents in which personal data have been processed, or is it sufficient if a full summary, in an intelligible form, of the personal data that have undergone processing in the documents concerned is provided?  
2.       Should the words “right of access” in Article 8(2) of [the Charter] be interpreted to mean that there is a right to a copy of documents in which personal data have been processed, or is it sufficient if there is provision of a full summary, in an intelligible form, of the personal data that have undergone processing in the documents concerned within the meaning of the second indent of Article 12(a) of [Directive 95/46]?  
3.       Is Article 41(2)(b) of [the Charter] also addressed to the Member States of the European Union in so far as they are implementing EU law within the meaning of Article 51(1) of that Charter?  
4.       Does the consequence that, as a result of the granting of access to “minutes”, the reasons why a particular decision is proposed are no longer recorded therein, which is not in the interests of the internal undisturbed exchange of views within the public authority concerned and of orderly decision-making, constitute a legitimate interest of confidentiality within the meaning of Article 41(2)(b) of [the Charter]?  
5.       Can a legal analysis, as set out in a “minute”, be regarded as personal data within the meaning of Article 2(a) of [Directive 95/46]?  
6.       Does the protection of the rights and freedoms of others, within the meaning of Article 13(1)(g) of [Directive 95/46] …, also cover the interest in an internal undisturbed exchange of views within the public authority concerned? If the answer to that is in the negative, can that interest then be covered by Article 13(1)(d) or (f) of that directive?’  
32      By decision of 30 April 2013, Cases C-141/12 and C-372/12 were joined for the purposes of the oral procedure and of the judgment.  
   
Consideration of the questions referred  
   
The first and second questions in Case C-141/12 and the fifth question in Case C-372/12, concerning the concept of ‘personal data’  
33      By the first and second questions in Case C-141/12 and the fifth question in Case C-372/12, which it is appropriate to examine together, the referring courts ask, in essence, whether Article 2(a) of Directive 95/46 must be interpreted as meaning that the data relating to the applicant for a residence permit and the legal analysis included in the minute are ‘personal data’ within the meaning of that provision.  
34      Although all interested parties who adopted a view on this point consider that the data relating to the applicant for a residence permit included in the minute correspond to the concept of ‘personal data’ and propose, consequently, that a positive reply be given to the first question in Case C-141/12, opinions differ in relation to the legal analysis in that administrative document, which is the subject of the second question in that case and the fifth question in Case C-372/12.  
35      YS, M and S, the Greek, Austrian and Portuguese Governments and the European Commission consider that, in so far as the legal analysis refers to a specific natural person and is based on the situation and that person’s individual characteristics, it also comes under the concept of ‘personal data’. The Greek Government and the Commission state, however, that that applies solely to legal analyses which contain information concerning an individual and not to those which contain only an abstract legal interpretation, while M and S consider that even such an abstract interpretation falls within the scope of that provision if it is decisive for the assessment of the application for a residence permit and is applied to the specific case of the applicant.  
36      By contrast, according to the Netherlands, Czech and French Governments, the legal analysis in a minute does not come under the concept of ‘personal data’.  
37      In this respect, it should be noted that Article 2(a) of Directive 95/46 defines personal data as ‘any information relating to an identified or identifiable natural person’.  
38      There is no doubt that the data relating to the applicant for a residence permit and contained in a minute, such as the applicant’s name, date of birth, nationality, gender, ethnicity, religion and language, are information relating to that natural person, who is identified in that minute in particular by his name, and must consequently be considered to be ‘personal data’ (see, to that effect, inter alia the judgment in   
Huber  
, C-524/06, EU:C:2008:724, paragraphs 31 and 43).  
39      As regards, on the other hand, the legal analysis in a minute, it must be stated that, although it may contain personal data, it does not in itself constitute such data within the meaning of Article 2(a) of Directive 95/46.  
40      As the Advocate General noted in essence in point 59 of her Opinion, and as the Netherlands, Czech and French Governments noted, such a legal analysis is not information relating to the applicant for a residence permit, but at most, in so far as it is not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant’s situation, that situation being established inter alia by means of the personal data relating to him which that authority has available to it.  
41      That interpretation of the concept of ‘personal data’ for the purposes of Directive 95/46 not only follows from the wording of Article 2(a) but is also borne out by the objective and general scheme of that directive.  
42      In accordance with Article 1 of that directive, its purpose is to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data, and thus to permit the free flow of personal data between Member States.  
43      According to recital 25 in the preamble to Directive 95/46, the principles of protection of natural persons provided therein are reflected, on the one hand, in the obligations imposed on those responsible for processing data concerning those persons and, on the other hand, in the rights conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.  
44      As regards those rights of the data subject, referred to in Directive 95/46, it must be noted that the protection of the fundamental right to respect for private life means, inter alia, that that person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner. As is apparent from recital 41 in the preamble to that directive, it is in order to carry out the necessary checks that the data subject has, under Article 12(a) of the directive, a right of access to the data relating to him which are being processed. That right of access is necessary, inter alia, to enable the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of his data by the controller and consequently to exercise the right set out in Article 12(b) of that directive (see, to that effect, the judgment in   
Rijkeboer  
, C-553/07, EU:C:2009:293, paragraphs 49 and 51).  
45      In contrast to the data relating to the applicant for a residence permit which is in the minute and which may constitute the factual basis of the legal analysis contained therein, such an analysis, as the Netherlands and French Governments have noted, is not in itself liable to be the subject of a check of its accuracy by that applicant and a rectification under Article 12(b) of Directive 95/46.  
46      In those circumstances, extending the right of access of the applicant for a residence permit to that legal analysis would not in fact serve the directive’s purpose of guaranteeing the protection of the applicant’s right to privacy with regard to the processing of data relating to him, but would serve the purpose of guaranteeing him a right of access to administrative documents, which is not however covered by Directive 95/46.  
47      In an analogous context, as regards the processing of personal data by the EU institutions, governed on the one hand by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1), and on the other by Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ 2001 L 145, p. 43), the Court has previously held, in paragraph 49 of the judgment in   
Commission   
v  
 Bavarian Lager  
, C-28/08 P, EU:C:2010:378, that those regulations have different objectives and that, in contrast to Regulation No 1049/2001, Regulation No 45/2001 is not designed to ensure the greatest possible transparency of the decision-making process of the public authorities and to promote good administrative practices by facilitating the exercise of the right of access to documents. That finding applies equally to Directive 95/46, which, in essence, has the same objective as Regulation No 45/2001.  
48      It follows from all the foregoing considerations that the answer to the first and second questions in Case C-141/12 and the fifth question in Case C-372/12 is that Article 2(a) of Directive 95/46 must be interpreted as meaning that the data relating to the applicant for a residence permit contained in the minute and, where relevant, the data in the legal analysis contained in the minute are ‘personal data’ within the meaning of that provision, whereas, by contrast, that analysis cannot in itself be so classified.  
   
The sixth question in Case C-372/12, concerning the possibility of limiting the right of access  
49      In the light of the answer given to the first and second questions in Case C-141/12 and to the fifth question in Case C-372/12, and since the referring court specified that the sixth question raised in Case C-372/12 requires an answer only if the legal analysis in the minute must be classified as personal data, there is no need to answer that sixth question.  
   
The third and fifth questions in Case C-141/12 and the first and second questions in Case C-372/12, concerning the scope of the right of access  
50      By the third and fifth questions in Case C-141/12 and by the first and second questions in Case C-372/12, which it is appropriate to examine together, the referring courts ask, in essence, whether Article 12(a) of Directive 95/46 and Article 8(2) of the Charter must be interpreted as meaning that the applicant for a residence permit has a right of access to data concerning him which are in the minute and, if so, whether that right to access implies that the competent authorities must provide him with a copy of that minute or whether it is sufficient for them to send him a full summary of those data in an intelligible form.  
51      All the parties to the proceedings before the Court agree that Article 12(a) of Directive 95/46 grants an applicant for a residence permit a right of access to all the personal data contained in the minute, although their views as regards the actual extent of that right differ according to their interpretation of the concept of ‘personal data’.  
52      As regards the form that that access must take, YS, M and S and the Greek Government consider that the applicant has the right to obtain a copy of the minute. They maintain that only such a copy would allow him to ensure that he is in possession of all the personal data which concern him in the minute.  
53      By contrast, according to the Netherlands, Czech, French and Portuguese Governments and the Commission, neither Article 12(a) of Directive 95/46 nor Article 8(2) of the Charter requires Member States to provide a copy of the minute to the applicant for a residence permit. Thus, there are other possible ways of disclosing, in an intelligible form, the personal data contained in such a document, inter alia by providing him with a full and comprehensible summary of those data.  
54      As a preliminary point, it should be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law of the Court, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter (see, inter alia, the judgments in   
Connolly   
v  
 Commission  
, C-274/99 P, EU:C:2001:127, paragraph 37;   
Österreichischer Rundfunk and Others  
, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; and   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 68).  
55      Article 8 of the Charter, which guarantees the right to the protection of personal data, provides in paragraph 2, inter alia, that everyone has the right of access to data which have been collected concerning him or her. That requirement is implemented by Article 12(a) of Directive 95/46 (see, to that effect, the judgment in   
Google Spain and Google  
, EU:C:2014:317, paragraph 69).  
56      That provision of Directive 95/46 provides that Member States are to guarantee every data subject the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay or expense, communication to him in an intelligible form of the data undergoing processing and of any available information as to their source.  
57      Although Directive 95/46 requires Member States to ensure that every data subject can obtain from the controller of personal data communication of all such data processed by the controller relating to the data subject, it leaves it to the Member States to determine the actual material form that that communication must take, as long as it is ‘intelligible’, in other words it allows the data subject to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that that person may, where relevant, exercise the rights conferred on him by Articles 12(b) and (c), 14, 22 and 23 of the directive (see, to that effect, the judgment in   
Rijkeboer  
, EU:C:2009:293, paragraphs 51 and 52).  
58      Therefore, in so far as the objective pursued by that right of access may be fully satisfied by another form of communication, the data subject cannot derive from either Article 12(a) of Directive 95/46 or Article 8(2) of the Charter the right to obtain a copy of the document or the original file in which those data appear. In order to avoid giving the data subject access to information other than the personal data relating to him, he may obtain a copy of the document or the original file in which that other information has been redacted.  
59      In situations such as those in the main proceedings, it follows from the answer given in paragraph 48 above that only the data relating to the applicant for a residence permit contained in the minute and, where relevant, the data in the legal analysis contained in the minute are ‘personal data’ within the meaning of Article 2(a) of Directive 95/46. Consequently the right of access which that applicant may rely on under Article 12(a) of Directive 95/46 and Article 8(2) of the Charter relates solely to those data. For that right of access to be complied with, it is sufficient for the applicant for a residence permit to be provided with a full summary of all of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him by Articles 12(b) and (c), 14, 22 and 23 of that directive.  
60      It follows from the foregoing considerations that the answer to the third and fifth questions in Case C-141/12 and the first and second questions in Case C-372/12 is that Article 12(a) of Directive 95/46 and Article 8(2) of the Charter must be interpreted as meaning that an applicant for a residence permit has a right of access to all personal data concerning him which are processed by the national administrative authorities within the meaning of Article 2(b) of that directive. For that right to be complied with, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him by that directive.  
   
The fourth question in Case C-141/12 and the third and fourth questions in Case C-372/12, concerning Article 41 of the Charter  
61      By the fourth question in Case C-141/12 and the third and fourth questions in Case C-372/12, which it is appropriate to examine together, the referring courts ask, in essence, whether Article 41(2)(b) of the Charter must be interpreted as meaning that the applicant for a residence permit may rely against national authorities on the right of access to the file provided for in that provision and, if so, what is the scope of the phrase ‘while respecting the legitimate interests of confidentiality’ in decision-making within the meaning of that provision.  
62      The Commission considers that those questions are inadmissible on account of their hypothetical and obscure wording.  
63      It should be borne in mind that, according to settled case-law of the Court, questions on the interpretation of EU law referred by a national court in the factual and legislative context which that court is responsible for defining, and the accuracy of which is not a matter for the Court to determine, enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see, inter alia, the judgment in   
Márquez Samohano  
, C-190/13, EU:C:2014:146, paragraph 35 and the case-law cited).  
64      However, that is not so in the present case. In the light of the factual context outlined by the referring courts, it does not appear that the question of whether the applicants in the main proceedings may, pursuant to Article 41(2)(b) of the Charter, rely on a right of access to the file concerning their applications for a residence permit is of a purely hypothetical nature. The wording of the questions and the information concerning them in the orders for reference are, furthermore, sufficiently clear to determine the scope of those questions and to enable, first, the Court to answer them and, secondly, the interested parties to submit their observations pursuant to Article 23 of the Statute of the Court of Justice of the European Union.  
65      On the substance of the questions referred, YS, M and S as well as the Greek Government consider that the applicant for a resident permit may take Article 41(2)(b) of the Charter as a basis for a right of access to the file, given that, in the context of the procedure for granting such a permit, the national authorities apply the asylum directives. By contrast, the Netherlands, Czech, French, Austrian and Portuguese Governments and the Commission consider that Article 41 of the Charter is directed exclusively at the EU institutions and cannot, therefore, establish a right of access to a file in the context of a national procedure.  
66      It should be noted from the outset that Article 41 of the Charter, ‘Right to good administration’, states in paragraph 1 that every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the European Union. Article 41(2) specifies that that right includes the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy.  
67      It is clear from the wording of Article 41 of the Charter that it is addressed not to the Member States but solely to the institutions, bodies, offices and agencies of the European Union (see, to that effect, the judgment in   
Cicala  
, C-482/10, EU:C:2011:868, paragraph 28). Consequently, an applicant for a resident permit cannot derive from Article 41(2)(b) of the Charter a right to access the national file relating to his application.  
68      It is true that the right to good administration, enshrined in that provision, reflects a general principle of EU law (judgment in   
HN  
, C-604/12, EU:C:2014:302, paragraph 49). However, by their questions in the present cases, the referring courts are not seeking an interpretation of that general principle, but ask whether Article 41 of the Charter may, in itself, apply to the Member States of the European Union.  
69      Consequently, the answer to the fourth question in Case C-141/12 and the third and fourth questions in Case C-372/12 is that Article 41(2)(b) of the Charter must be interpreted as meaning that the applicant for a residence permit cannot rely on that provision against the national authorities.  
   
Costs  
70      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the data relating to an applicant for a residence permit contained in an administrative document, such as the ‘minute’ at issue in the main proceedings, setting out the grounds that the case officer puts forward in support of the draft decision which he is responsible for drawing up in the context of the procedure prior to the adoption of a decision concerning the application for such a permit and, where relevant, the data in the legal analysis contained in that document, are ‘personal data’ within the meaning of that provision, whereas, by contrast, that analysis cannot in itself be so classified.  
2.        
Article 12(a) of Directive 95/46 and Article 8(2) of the Charter of Fundamental Rights of the European Union must be interpreted as meaning that an applicant for a residence permit has a right of access to all personal data concerning him which are processed by the national administrative authorities within the meaning of Article 2(b) of that directive. For that right to be complied with, it is sufficient that the applicant be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that applicant to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him by that directive.  
3.        
Article 41(2)(b) of the Charter of Fundamental Rights of the European Union must be interpreted as meaning that the applicant for a residence permit cannot rely on that provision against the national authorities.

ID: 0998e4a0-b93d-4a3d-8bbb-c8eb9bd63d76

Judgment of 1 Oct 2015, C-230/14 (  
Weltimmo  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Territorial Scope   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Competence   
General data protection law   
 >   
Chapter VII - Cooperation and consistency   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Processing   
   
JUDGMENT OF THE COURT (Third Chamber)  
1 October 2015 (\*)  
(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Articles 4(1) and 28(1), (3) and (6) — Controller who is formally established in a Member State — Impairment of the right to the protection of personal data concerning natural persons in another Member State — Determination of the applicable law and the competent supervisory authority — Exercise of the powers of the supervisory authority — Power to impose penalties)  
In Case C-230/14,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Kúria (Hungary), made by decision of 22 April 2014, received at the Court on 12 May 2014, in the proceedings  
Weltimmo s. r. o.  
v  
Nemzeti Adatvédelmi és Információszabadság Hatóság,  
THE COURT (Third Chamber),  
composed of M. Ilešič, President of the Chamber, A. Ó Caoimh, C. Toader, E. Jarašiūnas and C.G. Fernlund (Rapporteur), Judges,  
Advocate General: P. Cruz Villalón,  
Registrar: I. Illéssy, Administrator,  
having regard to the written procedure and further to the hearing on 12 March 2015,  
after considering the observations submitted on behalf of:  
–        the Nemzeti Adatvédelmi és Információszabadság Hatóság, by A. Péterfalvi, acting as Agent, and by G. Dudás, ügyvéd,  
–        the Hungarian Government, by M. Z. Fehér, G. Koós and A. Pálfy, acting as Agents,  
–        the Polish Government, by B. Majczyna, M. Kamejsza and M. Pawlicka, acting as Agents,  
–        the Slovak Government, by B. Ricziová, acting as Agent,  
–        the United Kingdom Government, by M. Holt, acting as Agent, and by J. Holmes, Barrister,  
–        the European Commission, by A. Tokár, B. Martenczuk and J. Vondung, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 25 June 2015,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Articles 4(1)(a) and 28(1), (3) and (6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Weltimmo s. r. o. (‘Weltimmo’), a company which has its registered office in Slovakia, and the Nemzeti Adatvédelmi és Információszabadság Hatóság (the national authority for data protection and freedom of information; ‘the Hungarian data protection authority’) concerning a fine imposed by the latter for infringement of Law CXII of 2011 on the right to self-determination as regards information and freedom of information (az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény; ‘the Law on information’), which transposed Directive 95/46 into Hungarian law.  
   
Legal context  
   
EU law  
3        Recitals 3, 18 and 19 in the preamble to Directive 95/46 state:  
‘(3)      Whereas the establishment and functioning of an internal market in which, in accordance with Article [26 TFEU], the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;  
…  
(18)      Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;  
(19)      Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities’.  
4        Article 2 of Directive 95/46 provides:  
‘For the purposes of this Directive:  
…  
(b)      “processing of personal data [‘feldolgozása’]” (“processing [‘feldolgozás’]”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;   
…’  
5        Article 4(1)(a) of Directive 95/46 provides:  
‘1.      Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:  
(a)      the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable’.  
6        According to Article 28(1), (3) and (6) of Directive 95/46:   
‘1.      Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.  
These authorities shall act with complete independence in exercising the functions entrusted to them.  
…  
3.      Each authority shall in particular be endowed with:  
–        investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,  
–        effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,  
–        the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.  
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.  
…  
6.      Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.  
The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.’  
   
Hungarian law  
7        Paragraph 2(1) of the Law on information provides:  
‘This Law shall apply to all data processing operations and technical manipulation of data carried out in the territory of Hungary that pertain to the data of natural persons or to public information or information of public interest.’  
8        Paragraph 3(10) and (17) of the Law on information contains the following definitions:  
‘(10)          “data processing” shall mean any operation or set of operations that is performed upon data, whether or not by automatic means, such as in particular collection, recording, organisation, storage, adaptation or alteration, use, retrieval, transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and blocking them from further use, photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images);  
…  
(17)      “technical manipulation of data” [“adatfeldolgozás”] shall mean the technical operations involved in data processing, irrespective of the method and instruments employed for such operations and the venue where it takes place, provided that such technical operations are carried out on the data. ’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
9        Weltimmo, a company registered in Slovakia, runs a property dealing website concerning Hungarian properties. For that purpose, it processes the personal data of the advertisers. The advertisements are free of charge for one month but thereafter a fee is payable. Many advertisers sent a request by e-mail for the deletion of both their advertisements and their personal data as from that period. However, Weltimmo did not delete those data and charged the interested parties for the price of its services. As the amounts charged were not paid, Weltimmo forwarded the personal data of the advertisers concerned to debt collection agencies.  
10      Those advertisers lodged complaints with the Hungarian data protection authority. That authority declared that it was competent under Paragraph 2(1) of the Law on information, taking the view that the collection of the data concerned constituted processing of data or a technical operation for the processing of data concerning natural persons. Considering that Weltimmo had infringed the Law on information, that data protection authority imposed on that company a fine of HUF 10 million (approximately EUR 32 000).  
11      Weltimmo then brought an action before the Budapest administrative and labour court (Fővárosi Közigazgatási és Munkaügyi Bíróság), which held that the fact that that company did not have a registered office or branch in Hungary was not a valid argument in defence because the processing of data and the supply of data services relating to the Hungarian property concerned had taken place in Hungary. However, that court set aside the decision of the Hungarian data protection authority on other grounds, connected with the lack of clarity over some of the facts.   
12      Weltimmo appealed on a point of law to the referring court, claiming that there was no need for further clarification of the facts, since, pursuant to Article 4(1)(a) of Directive 95/46, the Hungarian data protection authority in this case was not competent and could not apply Hungarian law in respect of a supplier of services established in another Member State. Weltimmo maintained that, under Article 28(6) of Directive 95/46, that authority should have asked the Slovak data protection authority to act in its place.  
13      The Hungarian data protection authority submitted that Weltimmo had a Hungarian representative in Hungary, namely one of the owners of that company, who represented it in the administrative and judicial proceedings that took place in that Member State. That authority added that Weltimmo’s Internet servers were probably installed in Germany or in Austria, but that the owners of that company lived in Hungary. Lastly, according to that authority, it follows from Article 28(6) of Directive 95/46 that it was in any event competent to act, regardless of the applicable law.  
14      Since it had doubts concerning the determination of the applicable law and the powers of the Hungarian data protection authority under Articles 4(1) and 28 of Directive 95/46, the Kúria (Supreme Court, Hungary) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Can Article 28(1) of Directive 95/46 be interpreted as meaning that the provisions of national law of a Member State are applicable in its territory to a situation where a data controller runs a property dealing website established only in another Member State and also advertises properties situated in the territory of that first Member State and the property owners have forwarded their personal data to a facility (server) for data storage and data processing belonging to the operator of the website in that other Member State?  
(2)      Can Article 4(1)(a) of [Directive 95/46], read in conjunction with recitals 18 to 20 of its preamble and Articles 1(2) and 28(1) thereof, be interpreted as meaning that the Hungarian [data protection authority] may not apply the Hungarian law on data protection, as national law, to an operator of a property dealing website established only in another Member State, even if it also advertises Hungarian property whose owners transfer the data relating to such property probably from Hungarian territory to a facility (server) for data storage and data processing belonging to the operator of the website?  
(3)      Is it significant for the purposes of interpretation that the service provided by the data controller who operates the website is directed at the territory of another Member State?  
(4)      Is it significant for the purposes of interpretation that the data relating to the properties in the other Member State and the personal data of the owners are uploaded in fact from the territory of that other Member State?  
(5)      Is it significant for the purposes of interpretation that the personal data relating to those properties are the personal data of citizens of another Member State?  
(6)      Is it significant for the purposes of interpretation that the owners of the undertaking established in Slovakia live in Hungary?  
(7)      If it appears from the answers to the above questions that the Hungarian data protection authority may act but must apply the law of the Member State of establishment and may not apply national law, must Article 28(6) of [Directive 95/46] be interpreted as meaning that the Hungarian data protection authority may only exercise the powers provided for by Article 28(3) of [Directive 95/46] in accordance with the provisions of the legislation of the Member State of establishment and accordingly may not impose a fine?  
(8)      May the term “adatfeldolgozás” (technical manipulation of data) used in both Article 4(1)(a) and in Article 28(6) of the [Hungarian version of Directive 95/46 to translate ‘data processing’] be considered to be equivalent to the usual term for data processing, “adatkezelés”, used in connection with that directive?’  
   
Consideration of the questions referred   
   
Preliminary observations  
15      As regards, first of all, the factual context of the main proceedings, certain additional information, which was submitted by the Hungarian data protection authority in its written observations and at the hearing before the Court, should be mentioned.  
16      It is apparent from that information, first, that that authority informally learned from its Slovak counterpart that Weltimmo did not carry out any activity at the place where it has its registered office, in Slovakia. Moreover, on several occasions, Weltimmo moved that registered office from one State to another. Secondly, Weltimmo developed two property dealing websites, written exclusively in Hungarian. It opened a bank account in Hungary, which was intended for the recovery of its debts, and had a letter box in that Member State for its everyday business affairs. The post was regularly picked up and sent to Weltimmo by electronic means. Thirdly, the advertisers themselves not only had to enter the data relating to their properties on Weltimmo’s website, but also had to delete those data from that website if they did not want those data to continue to appear on the website after the end of the one-month period mentioned above. Weltimmo raised a computer management issue in order to explain why it had not been possible to carry out that erasure. Fourthly, Weltimmo is a company made up of only one or two persons. Its representative in Hungary tried to negotiate the settlement of the unpaid debts with the advertisers.   
17      As regards, next, the wording of the questions referred, although the referring court uses the words ‘established only’ in its first and second questions, it is apparent from the order for reference and the written and oral observations submitted by the Hungarian data protection authority that, whilst Weltimmo is registered in Slovakia and is therefore established in that Member State, within the meaning of company law, there is uncertainty as to whether it is ‘established’ only in that Member State, within the meaning of Article 4(1)(a) of Directive 95/46. By referring a question to the Court regarding the interpretation of that provision, the referring court seeks to ascertain what is covered by the concept of ‘establishment’ used in that provision.  
18      Lastly, it must be observed that, in the first and second questions, the referring court mentions that the server used by Weltimmo is installed in Slovakia, whereas, in another passage in the order for reference, it mentions the possibility that that company’s servers may be in Germany or in Austria. In those circumstances, it seems appropriate to consider that the question as to the Member State in which the server or servers used by that company are installed is not settled.   
   
The first to sixth questions  
19      By its first to sixth questions, which should be examined together, the referring court asks, in essence, whether Articles 4(1)(a) and 28(1) of Directive 95/46 must be interpreted as permitting, in circumstances such as those at issue in the main proceedings, the data protection authority of a Member State to apply its national law on data protection with regard to a data controller whose company is registered in another Member State and who runs a property dealing website concerning properties situated in the territory of the first of those two States. In particular, the referring court asks whether it is significant that that Member State is the Member State:   
–        at which the activity of the controller of the personal data is directed,   
–        where the properties concerned are situated,  
–        from which the data of the owners of those properties are forwarded,  
–        of which those owners are nationals, and  
–        in which the owners of that company live.  
20      As regards the applicable law, the referring court refers in particular to Slovak and Hungarian law, Slovak law being the law of the Member State in which the controller of the personal data concerned is registered and Hungarian law being the law of the Member State mentioned by the websites at issue in the main proceedings, in the territory of which the properties forming the subject-matter of the published advertisements are situated.  
21      In that regard, it should be noted that Article 4 of Directive 95/46, entitled ‘National law applicable’, which is found in the first Chapter of that directive, entitled ‘General provisions’, specifically governs the question raised.   
22      By contrast, Article 28 of Directive 95/46, entitled ‘Supervisory authority’, deals with the role and powers of that authority. Pursuant to Article 28(1) of Directive 95/46, that authority is responsible for monitoring the application, within the territory of its own Member State, of the provisions adopted by the Member States pursuant to that directive. In accordance with Article 28(6) of that directive, the supervisory authority exercises the powers conferred on it, whatever the national law applicable to the processing of personal data.  
23      The national law applicable to the controller in respect of that processing must therefore be determined not in the light of Article 28 of Directive 95/46, but in the light of Article 4 of that directive.  
24      As set out in Article 4(1)(a) of Directive 95/46, each Member State is to apply the national provisions it adopts pursuant to that directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.  
25      In the light of the objective pursued by Directive 95/46, consisting in ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, the words ‘in the context of the activities of an establishment’ cannot be interpreted restrictively (see, to that effect, judgment in   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 53).  
26      In order to achieve that objective and to ensure that individuals are not deprived of the protection to which they are entitled under that directive, recital 18 in the preamble to that directive states that any processing of personal data in the European Union must be carried out in accordance with the law of one of the Member States and that processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State.   
27      The EU legislature thus prescribed a particularly broad territorial scope of Directive 95/46, which it registered in Article 4 thereof (see, to that effect, judgment in   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 54).  
28      With regard, in the first place, to the concept of ‘establishment’, it should be noted that recital 19 in the preamble to Directive 95/46 states that establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements and that the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor (judgment in   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 48). Moreover, that recital states that, when a single controller is established on the territory of several Member States, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.  
29      As the Advocate General observed, in essence, in points 28 and 32 to 34 of his Opinion, this results in a flexible definition of the concept of ‘establishment’, which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, in order to establish whether a company, the data controller, has an establishment, within the meaning of Directive 95/46, in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet.   
30      In that regard, it must, in particular, be held, in the light of the objective pursued by that directive, consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question.   
31      In addition, in order to attain that objective, it should be considered that the concept of ‘establishment’, within the meaning of Directive 95/46, extends to any real and effective activity — even a minimal one — exercised through stable arrangements.  
32      In the present case, the activity exercised by Weltimmo consists, at the very least, of the running of one or several property dealing websites concerning properties situated in Hungary, which are written in Hungarian and whose advertisements are subject to a fee after a period of one month. It must therefore be held that that company pursues a real and effective activity in Hungary.   
33      Furthermore, it is apparent in particular from the information provided by the Hungarian data protection authority that Weltimmo has a representative in Hungary, who is mentioned in the Slovak companies register with an address in Hungary and who has sought to negotiate the settlement of the unpaid debts with the advertisers. That representative served as a point of contact between that company and the data subjects who lodged complaints and represented the company in the administrative and judicial proceedings. In addition, that company has opened a bank account in Hungary, intended for the recovery of its debts, and uses a letter box in that Member State for the management of its everyday business affairs. That information, which it is for the referring court to verify, is capable of establishing, in a situation such as that at issue in the main proceedings, the existence of an ‘establishment’ within the meaning of Article 4(1)(a) of Directive 95/46.   
34      In the second place, it is necessary to establish whether the processing of personal data at issue is carried out ‘in the context of the activities’ of that establishment.   
35      The Court has already held that Article 4(1)(a) of Directive 95/46 requires the processing of personal data in question to be carried out not ‘by’ the establishment concerned itself, but only ‘in the context of the activities’ of the establishment (judgment in   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 52).  
36      In the present case, the processing at issue in the main proceedings consists, inter alia, of the publication, on Weltimmo’s property dealing websites, of personal data relating to the owners of those properties and, in some circumstances, of the use of those data for the purpose of the invoicing of the advertisements after a period of one month.   
37      In this respect, it should be observed that, as regards in particular the Internet, the Court has already had occasion to state that the operation of loading personal data on an Internet page must be considered to be ‘processing’ within the meaning of Article 2(b) of Directive 95/46 (judgments in   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 25, and   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 26).  
38      There is no doubt that that processing takes place in the context of the activities, as described in paragraph 32 of this judgment, which Weltimmo pursues in Hungary.  
39      Therefore, subject to the checks referred to in paragraph 33 of this judgment, which it is for the referring court to carry out for the purpose of establishing, should that be the case, the existence of an establishment of the controller in Hungary, it must be held that that processing is carried out in the context of the activities of that establishment and that Article 4(1)(a) of Directive 95/46 permits, in a situation such as that at issue in the main proceedings, the application of the Hungarian law on the protection of personal data.   
40      By contrast, the fact that the owners of the properties forming the subject-matter of the advertisements have Hungarian nationality is of no relevance whatsoever for the purposes of determining the national law applicable to the processing of the data at issue in the main proceedings.  
41      In the light of all the foregoing considerations, the answer to the first to sixth questions is as follows:  
–        Article 4(1)(a) of Directive 95/46 must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out;  
–        in order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State’s language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned;  
–        by contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.   
   
The seventh question  
42      The seventh question is asked only in the event that the Hungarian data protection authority should consider that Weltimmo has, not in Hungary but in another Member State, an establishment, within the meaning of Article 4(1)(a) of Directive 95/46, performing activities in the context of which the processing of the personal data concerned is carried out.  
43      By that question, the referring court asks, in essence, whether, should the Hungarian data protection authority reach the conclusion that the law applicable to the processing of the personal data is not Hungarian law, but the law of another Member State, Article 28(1), (3) and (6) of Directive 95/46 should be interpreted as meaning that that authority would be able to exercise only the powers provided for by Article 28(3) of that directive, in accordance with the law of that other Member State, and would not be able to impose penalties.  
44      With regard, in the first place, to the competence of a supervisory authority to act in such a case, it must be observed that, under Article 28(4) of Directive 95/46, each supervisory authority is to hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data.  
45      Consequently, in a situation such as that at issue in the main proceedings, the Hungarian data protection authority may hear claims lodged by persons, such as the advertisers of properties at issue in the main proceedings, who consider themselves victims of unlawful processing of their personal data in the Member State in which they hold those properties.   
46      In the second place, it is necessary to examine what are the powers of that supervisory authority, in the light of Article 28(1), (3) and (6) of Directive 95/46.  
47      It follows from Article 28(1) of that directive that each supervisory authority established by a Member State is to ensure compliance, within the territory of that Member State, with the provisions adopted by the Member States pursuant to Directive 95/46.  
48      Pursuant to Article 28(3) of Directive 95/46, those supervisory authorities are in particular to be endowed with investigative powers, such as powers to collect all the information necessary for the performance of their supervisory duties, and effective powers of intervention, such as powers of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, or of warning or admonishing the data controller.   
49      In view of the non-exhaustive nature of the powers thus listed and the type of powers of intervention mentioned in that provision, as well as the discretion available to the Member States in transposing Directive 95/46, it should be considered that those powers of intervention may include the power to penalise the data controller by imposing on him, where appropriate, a fine.  
50      The powers granted to the supervisory authorities must be exercised in accordance with the procedural law of the Member State to which they belong.  
51      It is apparent from Article 28(1) and (3) of Directive 95/46 that each supervisory authority is to exercise all of the powers conferred on it on the territory of its own Member State in order to ensure, on that territory, compliance with data protection rules.  
52      That territorial application of the powers of each supervisory authority is confirmed in Article 28(6) of the directive, which states that each supervisory authority is competent, whatever the national law applicable, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with Article 28(3) of that directive. Article 28(6) of the directive also states that each authority may be requested to exercise its powers by an authority of another Member State and that the supervisory authorities are to cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.  
53      That provision is necessary in order to ensure the free flow of personal data in the European Union, whilst ensuring compliance with the rules aimed at protecting the privacy of natural persons laid down in Directive 95/46. In the absence of that provision, where the controller of personal data is subject to the law of a Member State, but infringes the right to the protection of the privacy of natural persons in another Member State, in particular by directing his activity at that other Member State without, however, being established there within the meaning of that directive, it would be difficult, or even impossible, for those persons to enforce their right to that protection.   
54      It thus follows from Article 28(6) of Directive 95/46 that the supervisory authority of a Member State, to which a complaint has been submitted, on the basis of Article 28(4) of that directive, by natural persons in relation to the processing of their personal data, may examine that complaint irrespective of the applicable law, and, consequently, even if the law applicable to the processing of the data concerned is that of another Member State.  
55      However, in that case, the powers of that authority do not necessarily include all of the powers conferred on it in accordance with the law of its own Member State.   
56      As the Advocate General observed in point 50 of his Opinion, it follows from the requirements derived from the territorial sovereignty of the Member State concerned, the principle of legality and the concept of the rule of law that the exercise of the power to impose penalties cannot take place, as a matter of principle, outside the legal limits within which an administrative authority is authorised to act subject to the law of its own Member State.   
57      Thus, when a supervisory authority receives a complaint, in accordance with Article 28(4) of Directive 95/46, that authority may exercise its investigative powers irrespective of the applicable law and before even knowing which national law is applicable to the processing in question. However, if it reaches the conclusion that the law of another Member State is applicable, it cannot impose penalties outside the territory of its own Member State. In such a situation, it must, in fulfilment of the duty of cooperation laid down in Article 28(6) of that directive, request the supervisory authority of that other Member State to establish an infringement of that law and to impose penalties if that law permits, based, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State.  
58      The supervisory authority to which such a complaint has been submitted may, in the context of that cooperation, find it necessary to carry out other investigations, on the instructions of the supervisory authority of the other Member State.   
59      It follows that, in a situation such as that at issue in the main proceedings, if the applicable law is that of a Member State other than Hungary, the Hungarian data protection authority will not be able to exercise the powers to impose penalties which Hungarian law has conferred on it.  
60      It follows from the foregoing considerations that the answer to the seventh question is that, where the supervisory authority of a Member State, to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46, reaches the conclusion that the law applicable to the processing of the personal data concerned is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority will be able to exercise the effective powers of intervention conferred on it in accordance with Article 28(3) of that directive only within the territory of its own Member State. Accordingly, it cannot impose penalties on the basis of the law of that Member State on the controller with respect to the processing of those data who is not established in that territory, but should, in accordance with Article 28(6) of that directive, request the supervisory authority within the Member State whose law is applicable to act.   
   
The eighth question  
61      By its eighth question, the referring court seeks an interpretation from the Court of the scope of the term ‘adatfeldolgozás’ (technical manipulation of data) used in particular in Article 4(1)(a) of Directive 95/46, relating to the determination of the applicable law, and in Article 28(6) of that directive, relating to the competence of the supervisory authority.  
62      It is apparent from Directive 95/46, in the Hungarian version thereof, that that version consistently uses the term ‘adatfeldolgozás’.  
63      The referring court states that, in particular in its provisions designed to implement the provisions of Directive 95/46 relating to the competence of the supervisory authorities, the Law on information uses the term ‘adatkezelés’ (data processing). However, as is apparent from Paragraph 3(10) of that law, that term has a broader meaning than that of the term ‘adatfeldolgozás’, defined in Paragraph 3(17) of that law, and encompasses the latter term.   
64      Whilst, according to its usual meaning and as is apparent from the Law on information, the term ‘adatfeldolgozás’ has a narrower meaning than the term ‘adatkezelés’, it must however be observed that the Hungarian version of Directive 95/46 defines the term ‘adatfeldolgozás’ in Article 2(b) thereof in a broad manner, corresponding to the term ‘adatkezelés’.   
65      It follows that the answer to the eighth question is that Directive 95/46 must be interpreted as meaning that the term ‘adatfeldolgozás’ (technical manipulation of data), used in the Hungarian version of that directive, in particular in Articles 4(1)(a) and 28(6) thereof, must be understood as having the same meaning as that of the term ‘adatkezelés’ (data processing).  
   
Costs  
66      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 4(1)(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out.  
In order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State’s language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned.  
By contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.  
2.        
Where the supervisory authority of a Member State, to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46, reaches the conclusion that the law applicable to the processing of the personal data concerned is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority will be able to exercise the effective powers of intervention conferred on it in accordance with Article 28(3) of that directive only within the territory of its own Member State. Accordingly, it cannot impose penalties on the basis of the law of that Member State on the controller with respect to the processing of those data who is not established in that territory, but should, in accordance with Article 28(6) of that directive, request the supervisory authority within the Member State whose law is applicable to act.  
3.        
Directive 95/46 must be interpreted as meaning that the term ‘adatfeldolgozás’ (technical manipulation of data), used in the Hungarian version of that directive, in particular in Articles 4(1)(a) and 28(6) thereof, must be understood as having the same meaning as that of the term ‘adatkezelés’ (data processing).

ID: 0c8f0a68-6d68-425b-9f27-22ad3287bcc6

of 6 Oct 2020, C-623/17 (  
Privacy International  
)  
E-privacy Directive   
 >   
Material scope   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Location data   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
   
JUDGMENT OF THE COURT (Grand Chamber)  
6 October 2020 (\*)  
(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Providers of electronic communications services – General and indiscriminate transmission of traffic data and location data – Safeguarding of national security – Directive 2002/58/EC – Scope – Article 1(3) and Article 3 – Confidentiality of electronic communications – Protection – Article 5 and Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Article 4(2) TEU)  
In Case C-623/17,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Investigatory Powers Tribunal (United Kingdom), made by decision of 18 October 2017, received at the Court on 31 October 2017, in the proceedings  
Privacy International  
v  
Secretary of State for Foreign and Commonwealth Affairs,  
Secretary of State for the Home Department,  
Government Communications Headquarters,  
Security Service,  
Secret Intelligence Service,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb and L.S. Rossi, Presidents of Chambers, J. Malenovský, L. Bay Larsen, T. von Danwitz (Rapporteur), C. Toader, K. Jürimäe, C. Lycourgos and N. Piçarra, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 9 and 10 September 2019,  
after considering the observations submitted on behalf of:  
–        Privacy International, by B. Jaffey QC and T. de la Mare QC, by D. Cashman, Solicitor, and by H. Roy, avocat,  
–        the United Kingdom Government, by Z. Lavery, D. Guðmundsdóttir and S. Brandon, acting as Agents, by G. Facenna QC and D. Beard QC, and by C. Knight and R. Palmer, Barristers,  
–        the Belgian Government, by P. Cottin and J.-C. Halleux, acting as Agents, and by J. Vanpraet, advocaat, and E. de Lophem, avocat,  
–        the Czech Government, by M. Smolek, J. Vláčil and O. Serdula, acting as Agents,  
–        the German Government, initially by M. Hellmann, R. Kanitz, D. Klebs and T. Henze, and subsequently by J. Möller, M. Hellmann, R. Kanitz and D. Klebs, acting as Agents,  
–        the Estonian Government, by A. Kalbus, acting as Agent,  
–        Ireland, by M. Browne, G. Hodge and A. Joyce, acting as Agents, and by D. Fennelly, Barrister,  
–        the Spanish Government, initially by L. Aguilera Ruiz and M.J. García-Valdecasas Dorrego, and subsequently by L. Aguilera Ruiz, acting as Agents,  
–        the French Government, initially by E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas and D. Dubois, and subsequently by E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune and D. Dubois, acting as Agents,  
–        the Cypriot Government, by E. Symeonidou and E. Neofytou, acting as Agents,  
–        the Latvian Government, initially by V. Soņeca and I. Kucina, and subsequently by V. Soņeca, acting as Agents,  
–        the Hungarian Government, initially by G. Koós, M.Z. Fehér, G. Tornyai and Z. Wagner, and subsequently by G. Koós and M.Z. Fehér, acting as Agents,  
–        the Netherlands Government, by C.S. Schillemans and M.K. Bulterman, acting as Agents,  
–        the Polish Government, by B. Majczyna, J. Sawicka and M. Pawlicka, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes, M. Figueiredo and F. Aragão Homem, acting as Agents,  
–        the Swedish Government, initially by A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren and A. Alriksson, and subsequently by H. Shev, C. Meyer-Seitz, L. Zettergren and A. Alriksson, acting as Agents,  
–        the Norwegian Government, by T.B. Leming, M. Emberland and J. Vangsnes, acting as Agents,  
–        the European Commission, initially by H. Kranenborg, M. Wasmeier, D. Nardi and P. Costa de Oliveira, and subsequently by H. Kranenborg, M. Wasmeier, and D. Nardi, acting as Agents,  
–        the European Data Protection Supervisor, by T. Zerdick and A. Buchta, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 15 January 2020,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 1(3) and Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), read in the light of Article 4(2) TEU and Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between Privacy International and the Secretary of State for Foreign and Commonwealth Affairs (United Kingdom), the Secretary of State for the Home Department (United Kingdom), Government Communications Headquarters (United Kingdom) (‘GCHQ’), the Security Service (United Kingdom) (‘MI5’) and the Secret Intelligence Service (United Kingdom) (‘MI6’) concerning the legality of legislation authorising the acquisition and use of bulk communications data by the security and intelligence agencies.  
   
Legal context  
   
European Union law  
   
Directive 95/46  
3        Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), was repealed, with effect from 25 May 2018, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1). Article 3 of that directive, entitled ‘Scope’, was worded as follows:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI [TEU] and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
   
Directive 2002/58  
4        Recitals 2, 6, 7, 11, 22, 26 and 30 of Directive 2002/58 state:  
‘(2)      This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by [the Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of [the Charter].  
…   
(6)      The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.  
(7)      In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.  
…   
(11)      Like [Directive 95/46], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, [signed in Rome on 4 November 1950], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.  
…   
(22)      The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.  
…   
(26)      The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data … may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber’s right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services … should also be erased or made anonymous ….  
…   
(30)      Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. …’  
5        Article 1 of Directive 2002/58, entitled ‘Scope and aim’, provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in [the European Union].  
2.      The provisions of this Directive particularise and complement [Directive 95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.  
3.      This Directive shall not apply to activities which fall outside the scope of [the TFEU], such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.’  
6        According to Article 2 of that directive, entitled ‘Definitions’:  
‘Save as otherwise provided, the definitions in [Directive 95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.  
The following definitions shall also apply:  
(a)      “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  
(c)      “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
…’  
7        Article 3 of that directive, entitled ‘Services concerned’, provides:  
‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in [the European Union], including public communications networks supporting data collection and identification devices.’  
8        Under Article 5 of Directive 2002/58, entitled ‘Confidentiality of the communications’:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
…   
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with [Directive 95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
9        Article 6 of Directive 2002/58, entitled ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…   
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.’  
10      Article 9 of that directive, entitled ‘Location data other than traffic data’, provides, in paragraph 1 thereof:  
‘Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …’  
11      Article 15 of that directive, entitled ‘Application of certain provisions of [Directive 95/46]’, states, in paragraph 1 thereof:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of [Directive 95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of [EU] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’  
   
Regulation 2016/679  
12      Article 2 of Regulation 2016/679 provides:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;  
…   
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.  
…’  
13      Article 4 of that regulation provides:  
‘For the purposes of this Regulation:  
…   
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…’  
14      Under Article 23(1) of that regulation:  
‘Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;  
(e)      other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;  
(f)      the protection of judicial independence and judicial proceedings;  
(g)      the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;  
(h)      a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);  
(i)      the protection of the data subject or the rights and freedoms of others;  
(j)      the enforcement of civil law claims.’  
15      Under Article 94(2) of Regulation 2016/679:  
‘References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of [Directive 95/46] shall be construed as references to the European Data Protection Board established by this Regulation.’  
   
United Kingdom law  
16      Section 94 of the Telecommunications Act 1984, in the version applicable to the facts in the main proceedings (‘the 1984 Act’), entitled ‘Directions in the interests of national security etc.’, provides:  
‘(1)      The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.  
(2)      If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.  
(2A)      The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.  
(3)      A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under Part 1 or Chapter 1 of Part 2 of the Communications Act 2003 and, in the case of a direction to a provider of a public electronic communications network, notwithstanding that it relates to him in a capacity other than as the provider of such a network.  
(4)      The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of [the] opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.  
(5)      A person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.  
…   
(8)      This section applies to [the Office of Communications (OFCOM)] and to providers of public electronic communications networks.’  
17      Section 21(4) and (6) of the Regulation of Investigatory Powers Act 2000 (‘the RIPA’) provides:  
‘(4) … “communications data” means any of the following—  
(a)      any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;  
(b)      any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—  
(i)      of any postal service or telecommunications service; or  
(ii)      in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;  
(c)      any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.  
…   
(6)      … “traffic data”, in relation to any communication, means—  
(a)      any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,  
(b)      any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,  
(c)      any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and  
(d)      any data identifying the data or other data as data comprised in or attached to a particular communication.  
…’  
18      Sections 65 to 69 of the RIPA lay down the rules on the functioning and jurisdiction of the Investigatory Powers Tribunal (United Kingdom). Under section 65 of the RIPA, a complaint may be made to the Investigatory Powers Tribunal if there is reason to believe that data has been acquired inappropriately.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
19      At the beginning of 2015, the existence of practices for the acquisition and use of bulk communications data by the various security and intelligence agencies of the United Kingdom, namely GCHQ, MI5 and MI6, was made public, including in a report by the Intelligence and Security Committee of Parliament (United Kingdom). On 5 June 2015, Privacy International, a non-governmental organisation, brought an action before the Investigatory Powers Tribunal (United Kingdom) against the Secretary of State for Foreign and Commonwealth Affairs, the Secretary of State for the Home Department and those security and intelligence agencies, challenging the lawfulness of those practices.  
20      The referring court examined the lawfulness of those practices in the light, first of all, of national law and the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (‘the ECHR’), and, subsequently, of EU law. In a judgment of 17 October 2016, that court held that the defendants in the main proceedings had acknowledged that those agencies acquired and used, in their activities, sets of bulk personal data, such as biographical data or travel data, financial or commercial information, communications data liable to include sensitive data covered by professional secrecy, or journalistic material. That data, obtained by various, possibly secret, means, would be analysed by cross-checking and by automated processing and could be disclosed to other persons and authorities and shared with foreign partners. In that context, the security and intelligence agencies would also use bulk communications data, acquired from providers of public electronic communications networks under, inter alia, directions issued by a Secretary of State on the basis of section 94 of the 1984 Act. GCHQ and MI5 have been doing this since 2001 and 2005 respectively.  
21      The referring court found that those measures for the acquisition and use of data were consistent with national law and, since 2015, subject to issues that remained under consideration concerning the proportionality of those measures and the transfer of data to third parties, with Article 8 ECHR. In that regard, it stated that evidence had been submitted to it concerning the applicable safeguards, in particular as regards the procedures for accessing and disclosing data outside the security and intelligence agencies, the arrangements for retaining data, and independent oversight arrangements.  
22      As regards the lawfulness of the acquisition and use measures at issue in the main proceedings in the light of EU law, the referring court examined, in a judgment of 8 September 2017, whether those measures fell within the scope of EU law and, if so, whether they were compatible with EU law. That court found, as regards bulk communications data, that the providers of electronic communications networks were required, under section 94 of the 1984 Act, should a Secretary of State issue directions to that effect, to provide the security and intelligence agencies with data collected in the course of their economic activity falling within the scope of EU law. However, that was not the case for the acquisition of other data obtained by those agencies without the use of such binding powers. On the basis of that finding, the referring court considered it necessary to refer questions to the Court in order to determine whether a regime such as that resulting from section 94 of the 1984 Act falls within the scope of EU law and, if so, whether and in what way the requirements laid down by the case-law resulting from the judgment of 21 December 2016,   
Tele2 Sverige   
and  
 Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970; ‘  
Tele2  
’) apply to that regime.  
23      In that regard, in its request for a preliminary ruling, the referring court states that, pursuant to section 94 of the 1984 Act, the Secretary of State may give providers of electronic communications services such general or specific directions as appear to him to be necessary in the interests of national security or relations with a foreign government. Referring to the definitions set out in section 21(4) and (6) of the RIPA, that court states that the data concerned includes traffic data and service use information, within the meaning of that provision, with only the content of communications being excluded. Such data and information make it possible, in particular, to know the ‘who, where, when and how’ of a communication. That data is transmitted to the security and intelligence agencies and retained by them for the purposes of their activities.  
24      According to the referring court, the regime at issue in the main proceedings differs from that resulting from the Data Retention and Investigatory Powers Act 2014, at issue in the case which gave rise to the judgment of 21 December 2016,   
Tele2   
(C-203/15 and C-698/15, EU:C:2016:970), since the latter regime provided for the retention of data by providers of electronic communications services and the making available of that data not only to security and intelligence agencies, in the interests of national security, but also to other public authorities, depending on their needs. Furthermore, that judgment concerned a criminal investigation, not national security.  
25      The referring court adds that the databases compiled by the security and intelligence agencies are subject to bulk, unspecific, automated processing, with the aim of discovering unknown threats. To that end, the referring court states that the sets of metadata thus compiled should be as comprehensive as possible, so as to have a ‘haystack’ in order to find the ‘needle’ hidden therein. As regards the usefulness of bulk data acquisition by those agencies and the techniques for consulting that data, that court refers in particular to the findings of the report drawn up on 19 August 2016 by David Anderson QC, then United Kingdom Independent Reviewer of Terrorism Legislation, who relied, when drawing up that report, on a review conducted by a team of intelligence specialists and on the testimony of security and intelligence agency officers.  
26      The referring court also states that, according to Privacy International, the regime at issue in the main proceedings is unlawful in the light of EU law, while the defendants in the main proceedings consider that the obligation to transfer data provided for by that regime, access to that data and its use do not fall within the competences of the European Union, in accordance, in particular, with Article 4(2) TEU, according to which national security remains the sole responsibility of each Member State.  
27      In that regard, the Investigatory Powers Tribunal considers, on the basis of the judgment of 30 May 2006,   
Parliament  
 v   
Council and Commission  
 (C-317/04 and C-318/04, EU:C:2006:346, paragraphs 56 to 59), concerning the transfer of passenger name record data for the purpose of protecting public security, that the activities of commercial undertakings in processing and transferring data for the purpose of protecting national security do not appear to fall within the scope of EU law. For the referring court, it is necessary to examine not whether the activity in question constitutes data processing, but only whether, in substance and effect, the purpose of such activity is to advance an essential State function, within the meaning of Article 4(2) TEU, through a framework established by the public authorities that relates to public security.  
28      Should the measures at issue in the main proceedings nevertheless fall within the scope of EU law, the referring court considers that the requirements set out in paragraphs 119 to 125 of the judgment of 21 December 2016,   
Tele2   
 (C-203/15 and C-698/15, EU:C:2016:970) appear inappropriate in the context of national security and would undermine the ability of the security and intelligence agencies to tackle some threats to national security.  
29      In those circumstances, the Investigatory Powers Tribunal decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘In circumstances where:  
(a)      the [security and intelligence agencies’] capabilities to use [bulk communications data] supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation;  
(b)      a fundamental feature of the [security and intelligence agencies’] use of [bulk communications data] is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of [those data] in one place. Its principal utility lies in swift target identification and development, as well as providing a basis for action in the face of imminent threat;  
(c)      the provider of an electronic communications network is not thereafter required to retain [the bulk communications data] (beyond the period of their ordinary business requirements), which [are] retained by the State (the [security and intelligence agencies]) alone;  
(d)      the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of [bulk communications data] by the [security and intelligence agencies] are consistent with the requirements of the ECHR; and  
(e)      the national court has found that the imposition of the requirements specified in [paragraphs 119 to 125 of the judgment of 21 December 2016,   
Tele2   
(C-203/15 and C-698/15, EU:C:2016:970)], if applicable, would frustrate the measures taken to safeguard national security by the [security and intelligence agencies], and thereby put the national security of the United Kingdom at risk;  
(1)      Having regard to Article 4 TEU and Article 1(3) of [Directive 2002/58], does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the [security and intelligence agencies] of a Member State fall within the scope of Union law and of [Directive 2002/58]?  
(2)      If the answer to Question (1) is “yes”, do any of the [requirements applicable to retained communications data, set out in paragraphs 119 to 125 of the judgment of 21 December 2016,   
Tele2  
 (C-203/15 and C-698/15, EU:C:2016:970)] or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, taking into account the essential necessity of the [security and intelligence agencies] to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements?’  
   
Consideration of the questions referred  
   
Question 1  
30      By its first question, the referring court asks, in essence, whether Article 1(3) of Directive 2002/58, read in the light of Article 4(2) TEU, is to be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive.  
31      In that regard, Privacy International argues, in essence, that, having regard to the guidance derived from the case-law of the Court of Justice as regards the scope of Directive 2002/58, both the acquisition of data by the security and intelligence agencies from those providers under section 94 of the 1984 Act and the use of that data by those agencies fall within the scope of that directive, whether that data is acquired by means of a transmission carried out in real-time or subsequently. In particular, it argues that the fact that the objective of protecting national security is explicitly listed in Article 15(1) of that directive does not mean that the directive does not apply to such situations, and that assessment is not affected by Article 4(2) TEU.  
32      By contrast, the United Kingdom, Czech and Estonian Governments, Ireland, and the French, Cypriot, Hungarian, Polish and Swedish Governments contend, in essence, that Directive 2002/58 does not apply to the national legislation at issue in the main proceedings, as the purpose of that legislation is to safeguard national security. They argue that the activities of the security and intelligence agencies are essential State functions relating to the maintenance of law and order and the safeguarding of national security and territorial integrity, and, accordingly, are the sole responsibility of the Member States, as attested to by, in particular, the third sentence of Article 4(2) TEU.  
33      According to those governments, Directive 2002/58 cannot therefore be interpreted as meaning that national measures concerning the safeguarding of national security fall within its scope. Article 1(3) of that directive defines the scope of that directive and excludes from that scope, as was previously provided in the first indent of Article 3(2) of Directive 95/46, activities concerning public security, defence, and State security. Those provisions reflect the allocation of competences laid down in Article 4(2) TEU and would be deprived of any practical effect if it were necessary for measures in the field of national security to meet the requirements of Directive 2002/58. Furthermore, the case-law of the Court derived from the judgment of 30 May 2006,   
Parliament  
 v   
Council and Commission  
 (C-317/04 and C-318/04, EU:C:2006:346), concerning the first indent of Article 3(2) of Directive 95/46 can be transposed to Article 1(3) of Directive 2002/58.  
34      In that regard, it should be stated that, under Article 1(1) thereof, Directive 2002/58 provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector.  
35      Article 1(3) of that directive excludes from its scope ‘activities of the State’ in specified fields, including activities in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters. The activities thus mentioned by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 32 and the case-law cited).  
36      In addition, Article 3 of Directive 2002/58 states that the directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices (‘electronic communications services’). Consequently, that directive must be regarded as regulating the activities of the providers of such services (judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788  
,   
paragraph 33 and the case-law cited).  
37      In that context, Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, ‘legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 [of that directive]’ (judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 71).  
38      Article 15(1) of Directive 2002/58 necessarily presupposes that the national legislative measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met. Further, such measures regulate, for the purposes mentioned in that provision, the activity of providers of electronic communications services (judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788  
,   
paragraph 34 and the case-law cited).  
39      It is in the light of, inter alia, those considerations that the Court has held that Article 15(1) of Directive 2002/58, read in conjunction with Article 3 thereof, must be interpreted as meaning that the scope of that directive extends not only to a legislative measure that requires providers of electronic communications services to retain traffic data and location data, but also to a legislative measure requiring them to grant the competent national authorities access to that data. Such legislative measures necessarily involve the processing, by those providers, of the data and cannot, to the extent that they regulate the activities of those providers, be regarded as activities characteristic of States, referred to in Article 1(3) of Directive 2002/58 (see, to that effect, judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788  
,   
paragraphs 35 and 37 and the case-law cited).  
40      Concerning a legislative measure such as section 94 of the 1984 Act, on the basis of which the competent authority may give the providers of electronic communications services a direction to disclose bulk data to the security and intelligence agencies by transmission, it should be noted that, pursuant to the definition provided in Article 4(2) of Regulation 2016/679, which, according to Article 2 of Directive 2002/58, read in conjunction with Article 94(2) of that regulation, is applicable, the concept of ‘the processing of personal data’ designates ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, … storage, … consultation, use, disclosure by transmission, dissemination or otherwise making available …’.  
41      It follows that the disclosure of personal data by transmission, like the storage or otherwise making available of data, constitutes processing for the purposes of Article 3 of Directive 2002/58 and, accordingly, falls within the scope of that directive (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 45).  
42      In addition, having regard to the considerations set out in paragraph 38 above and the general scheme of Directive 2002/58, an interpretation of that directive under which the legislative measures referred to in Article 15(1) thereof were excluded from the scope of that directive because the objectives which such measures must pursue overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that same directive would deprive Article 15(1) thereof of any practical effect (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 72 and 73).  
43      The concept of ‘activities’ referred to in Article 1(3) of Directive 2002/58 cannot therefore, as was noted, in essence, by the Advocate General in point 75 of his Opinion in Joined Cases   
La Quadrature du Net and Others  
 (C-511/18 and C-512/18, EU:C:2020:6), to which he makes reference in point 24 of his Opinion in the present case, be interpreted as covering the legislative measures referred to in Article 15(1) of that directive.  
44      Article 4(2) TEU, to which the governments listed in paragraph 32 above have made reference, cannot invalidate that conclusion. Indeed, according to the settled case-law of the Court, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law (see, to that effect, judgments of 4 June 2013,   
ZZ  
, C-300/11, EU:C:2013:363, paragraph 38 and the case-law cited; of 20 March 2018,   
Commission  
 v   
Austria (State printing office)  
, C-187/16, EU:C:2018:194, paragraphs 75 and 76; and of 2 April 2020,   
Commission  
 v   
Poland, Hungary and Czech Republic (Temporary mechanism for the relocation of applicants for international protection)  
, C-715/17, C-718/17 and C-719/17, EU:C:2020:257, paragraphs 143 and 170).  
45      It is true that, in the judgment of 30 May 2006,   
Parliament  
 v   
Council and Commission  
 (C-317/04 and C-318/04, EU:C:2006:346, paragraphs 56 to 59), the Court held that the transfer of personal data by airlines to the public authorities of a third country for the purpose of preventing and combating terrorism and other serious crimes did not, pursuant to the first indent of Article 3(2) of Directive 95/46, fall within the scope of that directive, because such a transfer fell within a framework established by the public authorities relating to public security.  
46      However, having regard to the findings set out in paragraphs 36, 38 and 39 above, that case-law cannot be transposed to the interpretation of Article 1(3) of Directive 2002/58. Indeed, as the Advocate General noted, in essence, in points 70 to 72 of his Opinion in Joined Cases   
La Quadrature du Net and Others  
 (C-511/18 and C-512/18, EU:C:2020:6), the first indent of Article 3(2) of Directive 95/46, to which that case-law relates, excluded, in a general way, from the scope of that directive ‘processing operations concerning public security, defence, [and] State security’, without drawing any distinction according to who was carrying out the data processing operation concerned. By contrast, in the context of interpreting Article 1(3) of Directive 2002/58, it is necessary to draw such a distinction. As is apparent from paragraphs 37 to 39 and 42 above, all operations processing personal data carried out by providers of electronic communications services fall within the scope of that directive, including processing operations resulting from obligations imposed on those providers by the public authorities, whereas those processing operations could, where appropriate, on the contrary, fall within the scope of the exception laid down in the first indent of Article 3(2) of Directive 95/46, given the broader wording of that provision, which covers all processing operations concerning public security, defence, or State security, regardless of the person carrying out those operations.  
47      Furthermore, it should be noted that Directive 95/46, which was at issue in the case that gave rise to the judgment of 30 May 2006,   
Parliament  
 v   
Council and Commission  
 (C-317/04 and C-318/04, EU:C:2006:346), has been, pursuant to Article 94(1) of Regulation 2016/679, repealed and replaced by that regulation with effect from 25 May 2018. Although that regulation states, in Article 2(2)(d) thereof, that it does not apply to processing operations carried out ‘by competent authorities’ for the purposes of, inter alia, the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security, it is apparent from Article 23(1)(d) and (h) of that regulation that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation. It follows that the above interpretation of Article 1(3), Article 3 and Article 15(1) of Directive 2002/58 is consistent with the definition of the scope of Regulation 2016/679, which is supplemented and specified by that directive.  
48      By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is not covered by Directive 2002/58, but by national law only, subject to the application of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89), with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR.  
49      Having regard to the foregoing considerations, the answer to the first question is that Article 1(3), Article 3 and Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU, must be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive.  
   
Question 2  
50      By its second question, the referring court seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter, is to be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.  
51      As a preliminary point, it should be borne in mind that, according to the information set out in the request for a preliminary ruling, section 94 of the 1984 Act permits the Secretary of State to require providers of electronic communications services, by way of directions, if he considers it necessary in the interests of national security or relations with a foreign government, to forward bulk communications data to the security and intelligence agencies. That data includes traffic data and location data, as well as information relating to the services used, pursuant to section 21(4) and (6) of the RIPA. That provision covers, inter alia, the data necessary to (i) identify the source and destination of a communication, (ii) determine the date, time, length and type of communication, (iii) identify the hardware used, and (iv) locate the terminal equipment and the communications. That data includes, inter alia, the name and address of the user, the telephone number of the person making the call and the number called by that person, the IP addresses of the source and addressee of the communication and the addresses of the websites visited.  
52      Such a disclosure of data by transmission concerns all users of means of electronic communication, without its being specified whether that transmission must take place in real-time or subsequently. Once transmitted, that data is, according to the information set out in the request for a preliminary ruling, retained by the security and intelligence agencies and remains available to those agencies for the purposes of their activities, as with the other databases maintained by those agencies. In particular, the data thus acquired, which is subject to bulk automated processing and analysis, may be cross-checked with other databases containing different categories of bulk personal data or be disclosed outside those agencies and to third countries. Lastly, those operations do not require prior authorisation from a court or independent administrative authority and do not involve notifying the persons concerned in any way.  
53      As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of Directive 2002/58 is to protect users of electronic communications services from risks for their personal data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, that directive seeks, as is stated in recital 2 thereof, to ensure that the rights set out in Articles 7 and 8 of the Charter are fully respected. In that regard, it is apparent from the Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM (2000) 385 final), which gave rise to Directive 2002/58, that the EU legislature sought to ‘ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used’.  
54      To that end, Article 5(1) of Directive 2002/58 provides that ‘Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation’. That provision also emphasises that, ‘in particular, [Member States] shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)’, and specifies that ‘this paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.’  
55      Thus, Article 5(1) of that directive enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires, inter alia, that, in principle, persons other than users be prohibited from storing, without those users’ consent, those communications and that data. Having regard to the general nature of its wording, that provision necessarily covers any operation enabling third parties to become aware of communications and data relating thereto for purposes other than the conveyance of a communication.  
56      The prohibition on the interception of communications and data relating thereto laid down in Article 5(1) of Directive 2002/58 therefore encompasses any instance of providers of electronic communications services making traffic data and location data available to public authorities, such as the security and intelligence agencies, as well as the retention of that data by those authorities, regardless of how that data is subsequently used.  
57      Thus, in adopting that directive, the EU legislature gave concrete expression to the rights enshrined in Articles 7 and 8 of the Charter, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, paragraph 109).  
58      However, Article 15(1) of Directive 2002/58 enables the Member States to introduce an exception to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to, inter alia, in Articles 6 and 9 of that directive, where this constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. To that end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on one of those grounds.  
59      That being said, the option to derogate from the rights and obligations laid down in Articles 5, 6 and 9 of Directive 2002/58 cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of that data, explicitly laid down in Article 5 of that directive, to become the rule (see judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 89 and 104, and judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, paragraph 111).  
60      In addition, it is apparent from the third sentence of Article 15(1) of Directive 2002/58 that the Member States are not permitted to adopt legislative measures to restrict the scope of the rights and obligations provided for in Articles 5, 6 and 9 of that directive unless they do so in accordance with the general principles of EU law, including the principle of proportionality, and with the fundamental rights guaranteed in the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making it available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (see, to that effect, judgments of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 25 and 70, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 91 and 92 and the case-law cited).  
61      Those same issues also arise for other types of data processing, such as the transmission of that data to persons other than users or access to that data with a view to its use (see, by analogy, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraphs 122 and 123 and the case-law cited).  
62      Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that that fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 6 March 2001,   
Connolly  
 v   
Commission  
, C-274/99 P, EU:C:2001:127, paragraph 39, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 93 and the case-law cited).  
63      However, the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 172 and the case-law cited).  
64      Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.  
65      It should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned ( judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited).  
66      Concerning observance of the principle of proportionality, the first sentence of Article 15(1) of Directive 2002/58 provides that the Member States may adopt a measure derogating from the principle that communications and the related traffic data are to be confidential where such a measure is ‘necessary, appropriate and proportionate … within a democratic society’, in view of the objectives set out in that provision. Recital 11 of that directive specifies that a measure of that nature must be ‘strictly’ proportionate to the intended purpose.  
67      In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (see, to that effect, judgments of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 56; of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 76, 77 and 86; and of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52; Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 140).  
68      In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, in particular where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake (see, to that effect, judgments of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 117; Opinion 1/15   
(EU-Canada PNR Agreement)   
of 26 July 2017, EU:C:2017:592, paragraph 141).  
69      As regards the question whether national legislation, such as that at issue in the main proceedings, meets the requirements of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, it should be noted that the transmission of traffic data and location data to persons other than users, such as security and intelligence agencies, derogates from the principle of confidentiality. Where that operation is carried out, as in the present case, in a general and indiscriminate way, it has the effect of making the exception to the obligation of principle to ensure the confidentiality of data the rule, whereas the system established by Directive 2002/58 requires that that exception remain an exception.  
70      In addition, in accordance with the settled case-law of the Court, the transmission of traffic data and location data to a third party constitutes interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, regardless of how that data is subsequently used. In that regard, it does not matter whether the information in question relating to persons’ private lives is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126 and the case-law cited, and judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, paragraphs 115 and 116).  
71      The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications. In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (see, by analogy, judgments of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 27 and 37, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 99 and 100).  
72      It should also be noted that the transmission of traffic data and location data to public authorities for security purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of means of electronic communication from exercising their freedom of expression, guaranteed in Article 11 of the Charter. Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistle-blowers whose actions are protected by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ 2019 L 305, p. 17). Moreover, that deterrent effect is all the more serious given the quantity and breadth of the data retained (see, to that effect, judgments of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 28; of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 101; and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, paragraph 118).  
73      Lastly, given the significant amount of traffic data and location data that can be retained continuously by a general retention measure and the sensitive nature of the information which that data may provide, the mere retention of that data by the providers of electronic communications services entails a risk of abuse and unlawful access.  
74      As regards the objectives that may justify such interferences, and in particular the objective of safeguarding national security, at issue in the main proceedings, it should be noted, at the outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, paragraph 135).  
75      The importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats such as those referred to in paragraph 74 above can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, paragraph 136).  
76      However, in order to satisfy the requirement of proportionality referred to in paragraph 67 above, according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, national legislation entailing interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter must meet the requirements stemming from the case-law cited in paragraphs 65, 67 and 68 above.  
77      In particular, as regards an authority’s access to personal data, legislation cannot confine itself to requiring that authorities’ access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, paragraph 192 and the case-law cited).  
78      Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the aim pursued, cannot be regarded as being limited to what is strictly necessary, national legislation governing access to traffic data and location data must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119 and the case-law cited).  
79      Those requirements apply, a fortiori, to a legislative measure, such as that at issue in the main proceedings, on the basis of which the competent national authority may require providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission. Such transmission has the effect of making that data available to the public authorities (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, paragraph 212).  
80      Given that the transmission of traffic data and location data is carried out in a general and indiscriminate way, it is comprehensive in that it affects all persons using electronic communications services. It therefore applies even to persons for whom there is no evidence to suggest that their conduct might have a link, even an indirect or remote one, with the objective of safeguarding national security and, in particular, without any relationship being established between the data which is to be transmitted and a threat to national security (see, to that effect, judgments of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 and 58, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 105). Having regard to the fact that the transmission of such data to public authorities is equivalent, in accordance with the finding in paragraph 79 above, to access, it must be held that legislation which permits the general and indiscriminate transmission of data to public authorities entails general access.  
81      It follows that national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter.  
82      In the light of all the foregoing considerations, the answer to the second question is that Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.  
   
Costs  
83      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 1(3), Article 3 and Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Article 4(2) TEU, must be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive.  
2.        
Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.  
Lenaerts  
Silva de Lapuerta  
Bonichot  
Arabadjiev  
Prechal  
Safjan  
Xuereb  
Rossi  
Malenovský  
Bay Larsen  
von Danwitz  
Toader  
Jürimäe  
Lycourgos  
Piçarra  
Delivered in open court in Luxembourg on 6 October 2020.  
A. Calot Escobar  
   
K. Lenaerts  
Registrar  
   
President  
\*      Language of the case: English.  
   
  
  
  
  
Disclaimer

ID: 0d2f74b9-684f-4d5b-a7c6-c666413238fb

of 2 Mar 2023, C-268/21 (  
Norra Stockholm Bygg  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legal obligation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
   
JUDGMENT OF THE COURT (Third Chamber)  
2 March 2023 (\*)  
(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 6(3) and (4) – Lawfulness of processing – Production of a document containing personal data in civil court proceedings – Article 23(1)(f) and (j) – Protection of judicial independence and judicial proceedings – Enforcement of civil law claims – Requirements to be complied with – Having regard to the interests of the data subjects – Balancing of the opposing interests involved – Article 5 – Minimisation of personal data – Charter of Fundamental Rights of the European Union – Article 7 – Right to respect for private life – Article 8 – Right to protection of personal data – Article 47 – Right to effective judicial protection – Principle of proportionality)  
In Case C-268/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Högsta domstolen (Supreme Court, Sweden), made by decision of 15 April 2021, received at the Court on 23 April 2021, in the proceedings  
Norra Stockholm Bygg AB  
v  
Per Nycander AB,  
other party:  
Entral AB,  
THE COURT (Third Chamber),  
composed of K. Jürimäe, President of the Chamber, M.L. Arasteyx² Sahún, N. Piçarra, N. Jääskinen (Rapporteur) and M. Gavalec, Judges,  
Advocate General: T. Ćapeta,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 27 June 2022,  
after considering the observations submitted on behalf of:  
–        Norra Stockholm Bygg AB, by H. Täng Nilsson and E. Wassén, advokater,  
–        Per Nycander AB, by P. Degerfeldt and V. Hermansson, advokater,  
–        the Swedish Government, by C. Meyer-Seitz and H. Shev, and by O. Simonsson, acting as Agents,  
–        the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
–        the Polish Government, by B. Majczyna and J. Sawicka, acting as Agents,  
–        the European Commission, by A. Bouchagiar, M. Gustafsson and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 6 October 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 6(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
2        The request has been made in proceedings between Norra Stockholm Bygg AB (‘Fastec’) and Per Nycander AB (‘Nycander’) concerning a request for disclosure of the electronic register of Fastec’s staff who had carried out work for Nycander, with a view to determining the amount of work to be paid by the latter.  
   
Legal context  
   
European Union law  
3        Recitals 1, 2, 4, 20, 26, 45 and 50 of the GDPR are worded as follows:  
‘(1)      The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the “Charter”) and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.  
(2)      The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.  
…  
(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. …  
…  
(20)      While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. …  
…  
(26)      The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. … The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. …  
…  
(45)      Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. … A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. …  
…  
(50)      The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. … The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. …  
Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. …’  
4        Article 2 of that regulation, entitled ‘Material scope’, provides:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;  
(c)      by a natural person in the course of a purely personal or household activity;  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.   
3.      For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 [of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1)] applies. Regulation [No 45/2001] and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.’  
5        Under Article 4 of the said regulation:  
‘For the purposes of this Regulation:  
…  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(5)      “pseudonymisation” means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;  
…’  
6        Article 5 of the same regulation, entitled ‘Principles relating to the processing of personal data’, states, in paragraph 1 thereof:  
‘Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … (“purpose limitation”);   
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);  
…’  
7        Article 6 of the GDPR, entitled ‘Lawfulness of processing’, provides:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
…  
3.      The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.  
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. … The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.  
4.      Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject’s consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:  
(a)      any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;  
…’  
8        Article 23 of that regulation, entitled ‘Restrictions’, provides:  
‘1.      Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
…  
(f)      the protection of judicial independence and judicial proceedings;  
…  
(j)      the enforcement of civil law claims.  
…’  
   
Swedish law  
   
The RB  
9        Documentary evidence is governed by the provisions of Chapter 38 of the rättegångsbalken (Code of Judicial Procedure; ‘the RB’).  
10      Under the first subparagraph of Paragraph 2 of Chapter 38 of the RB, any person in possession of a written document which may be deemed to have probative value is required to produce that document.  
11      Exceptions to that production obligation are provided for, inter alia, in the second subparagraph of that paragraph. The performance of certain functions dispenses with that obligation if it can be presumed that the person in possession of that document may not be heard as a witness on its content. That exception applies to lawyers, doctors, psychologists, priests and any other person to whom information has been disclosed in confidence in the performance of his or her functions or in similar circumstances. The scope of the said obligation thus corresponds to the obligation to stand as a witness in legal proceedings.  
12      If a person is required to produce a document as evidence, the court may, in accordance with Paragraph 4 of Chapter 38 of the RB, order him or her to do so.  
   
The Law on tax procedures  
13      Under Paragraphs 11a to 11c of Chapter 39 of the skatteförfarandelagen (2011:1244) [Law (2011:1244) on tax procedures], any person who carries on a construction activity is obliged, in certain cases, to maintain an electronic staff register. That staff register is to document the necessary identification data relating to the persons involved in that economic activity. That obligation is incumbent on the developer, which may, however, delegate it to an independent operator. By virtue of Paragraph 12 of Chapter 39 of that law, the staff register must be made available to the Swedish tax authority.  
14      The data which must be recorded in the staff register are set out in Paragraph 5 of Chapter 9 of the skatteförfarandeförordningen (2011:1261) [Regulation (2011:1261) on tax procedures]. These include the identity and national identification number of any person involved in the economic activity as well as the start and end times of work.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
15      Fastec constructed an office building for Nycander. The persons working on the building site concerned recorded their presence by means of an electronic staff register. That staff register was provided by the company Entral AB, acting on behalf of Fastec.  
16      Fastec brought an action before the tingsrätt (District Court, Sweden) seeking payment for the works carried out. In that action, Fastec requested Nycander to pay a sum which, according to Fastec, corresponds to the outstanding balance owed by Nycander. The latter company objected to Fastec’s request, claiming, inter alia, that the number of hours worked by Fastec’s staff was lower than that indicated in that request.  
17      Before that court, Nycander requested that Entral be ordered to produce Fastec’s staff register for the period from 1 August 2016 to 30 November 2017, primarily without redaction, or, in the alternative, with the personal identity numbers of the persons concerned redacted. In support of that request, Nycander claimed that Entral had that staff register in its possession and that it could constitute important evidence for the purposes of ruling on Fastec’s action in so far as the data recorded enabled the hours worked by Fastec’s staff to be proved.  
18      Fastec objected to that request, claiming, primarily, that it was contrary to Article 5(1)(b) of the GDPR. It stated that its staff register contains personal data collected in order for checks to be carried out on its activities by the Swedish tax authority, and disclosing those data to the court was not consistent with that objective.  
19      The tingsrätt (District Court) ordered Entral to produce in an unredacted state Fastec’s staff register for the staff concerned by the building site at issue in the main proceedings during the relevant period. The Svea hovrätten (Svea Court of Appeal, Stockholm, Sweden) upheld the decision of the tingsrätten (District Court).  
20      Fastec brought an appeal against the decision of the Svea hovrätt (Svea Court of Appeal, Stockholm) before the referring court, the Högsta domstolen (Supreme Court, Sweden), and asked that Nycander’s request referred to in paragraph 17 above be rejected.   
21      The referring court asks whether – and, if so, how – the provisions of the GDPR should be applied in the case in the main proceedings.   
22      So far as concerns the obligation to produce documents, that court observes that it is apparent from its own case-law on the interpretation of the relevant provisions of the RB that it is necessary to weigh up the relevance of the evidence at issue against the opposing party’s interest in not releasing that information. It states that, in the context of that weighing exercise, no account is taken, in principle, of whether the information contained in the document is private in nature or whether other persons have an interest in having access to the content of that document, aside from what may follow from the exceptions specifically provided for by the legislation.  
23      The referring court states that the purpose of the obligation to produce a document laid down by the RB is, inter alia, to give anyone who needs a written document as evidence access to it. In its view, it is ultimately a question of ensuring that individuals are able to exercise their rights where they have a ‘justified probative interest’.  
24      In those circumstances, the Högsta domstolen (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘1.      Does Article 6(3) and (4) of the GDPR also impose a requirement on national procedural legislation relating to [the obligation to produce documents]?  
2.      If Question 1 is answered in the affirmative, does the GDPR mean that regard must also be had to the interests of the data subjects when a decision on [production] must be made which involves the processing of personal data? In such circumstances, does EU law establish any requirements concerning how, in detail, that decision should be made?’  
   
Consideration of the questions referred  
   
The first question  
25      By its first question, the referring court asks, in essence, whether Article 6(3) and (4) of the GDPR must be interpreted as meaning that that provision applies, in the context of civil court proceedings, to the production as evidence of a staff register containing personal data of third parties collected principally for the purposes of tax inspection.  
26      In order to answer that question, it should be noted, in the first place, that Article 2(1) of the GDPR provides that that regulation applies to any ‘processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system’, without any distinction being made according to the identity of the person who carried out the processing concerned. It follows that, subject to the cases mentioned in Article 2(2) and (3) thereof, the GDPR applies to processing operations carried out both by private persons and by public authorities, including, as recital 20 thereof indicates, judicial authorities, such as courts (judgment of 24 March 2022,   
Autoriteit Persoonsgegevens  
, C-245/20, EU:C:2022:216, paragraph 25).   
27      In the second place, according to Article 4(2) of that regulation, the definition of ‘processing’ of personal data includes any operation which is performed on personal data, whether or not by automated means, such as collection, recording, use, disclosure by transmission, dissemination or otherwise making available.  
28      It follows that a processing operation which falls within the material scope of the GDPR includes not only the creation and maintenance of the electronic staff register (see, by analogy, judgment of 30 May 2013,   
Worten  
, C-342/12, EU:C:2013:355, paragraph 19), but also the production as evidence of a document, whether digital or physical, containing personal data, ordered by a court in the context of judicial proceedings (see, to that effect, judgment of 8 December 2022,   
Inspektor v Inspektorata kam Visshia sadeben savet (Purposes of processing personal data) – Criminal investigation)  
, C-180/21, EU:C:2022:967, paragraph 72).  
29      In the third place, it must be pointed out that any processing of personal data, including processing carried out by public authorities such as courts, must satisfy the conditions of lawfulness set by Article 6 of the GDPR.  
30      In that regard, it should be noted, first, that, according to Article 6(1)(e) of the GDPR, the processing of personal data is lawful if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.  
31      In accordance with Article 6(3) of the GDPR, read in combination with recital 45 thereof, the basis for the processing referred to in Article 6(1)(e) of that regulation is to be defined by EU law or by Member State law to which the controller is subject. Moreover, the EU or Member State law must meet an objective of public interest and be proportionate to the legitimate aim pursued.  
32      The combined provisions of Article 6(1)(e) of the GDPR and Article 6(3) thereof therefore require there to be a legal basis – national in particular – which serves as a basis for the processing of personal data by the relevant controllers acting in the performance of a task carried out in the public interest or in the exercise of official authority, such as those performed by courts acting in their judicial capacity.  
33      Second, where the processing of personal data is carried out for a purpose other than that for which those data have been collected, it follows from Article 6(4) of the GDPR, read in the light of recital 50 thereof, that such processing is allowed provided that it is based, inter alia, on Member State law and that it constitutes a necessary and proportionate measure in a democratic society to safeguard one of the objectives referred to in Article 23(1) of the GDPR. As that recital indicates, in order to safeguard those important objectives of general public interest, the controller is thus allowed to further process the personal data irrespective of the compatibility of that processing with the purposes for which the personal data were initially collected.  
34      In the case at hand, the relevant provisions of Chapter 38 of the RB, which lay down the obligation to produce a document as evidence and provide for the possibility for national courts to order the production of that document, constitute the legal basis serving as a basis for the processing of personal data. While those provisions constitute, in principle, a sufficient legal basis for allowing the processing of personal data, it is apparent from the order for reference that that legal basis is different from that constituted by the Law on tax procedures, on the basis of which the staff register at issue in the main proceedings was drawn up for the purposes of tax inspection. Moreover, the purpose of the obligation to produce documents laid down by those provisions of the RB is, according to the referring court, to give anyone who needs a written document as evidence access to it. In its view, it is a question of ensuring that individuals are able to exercise their rights where they have a ‘justified probative interest’.  
35      According to that court, it is apparent from the   
travaux préparatoires  
 that led to the Law on tax procedures that the personal data recorded in the staff register are intended to enable officials of the competent Swedish tax authority to carry out verifications during its on-site inspections. The essential objective is to reduce the occurrence of concealed work and to improve the conditions for competition. The processing of personal data is justified by the need to satisfy the legal obligation on the controller, namely to keep a staff register.  
36      Accordingly, it must be held that the processing of those data in the context of judicial proceedings such as the main proceedings constitutes processing carried out for a purpose other than that for which the data have been collected, namely for the purposes of tax inspection, and which is not based on the consent of the data subjects, within the meaning of Article 6(1)(a) of the GDPR.  
37      In those circumstances, the processing of personal data for a purpose other than that for which those data have been collected must not only be based on national law, such as the provisions of Chapter 38 of the RB, but also constitute a necessary and proportionate measure in a democratic society, within the meaning of Article 6(4) of the GDPR, and safeguard one of the objectives referred to in Article 23(1) of the GDPR.   
38      Those objectives include, in accordance with Article 23(1)(f) of that regulation, ‘the protection of judicial independence and judicial proceedings’, which, as the European Commission noted in its written observations, must be understood as referring to the protection of the administration of justice from internal or external interference, but also to the proper administration of justice. Furthermore, according to Article 23(1)(j) thereof, the enforcement of civil law claims also constitutes an objective which may justify the processing of personal data for a purpose other than that for which they have been collected. It cannot therefore be ruled out that the processing of personal data of third parties in civil court proceedings may be based on such objectives.  
39      However, it is for the referring court to ascertain whether the relevant provisions of Chapter 38 of the RB, first, meet one and/or other of those objectives and, second, are necessary and proportionate to the said objectives, so that they are capable of falling within the scope of cases of personal data processing regarded as lawful under the provisions of Article 6(3) and (4) of the GDPR, read in combination with Article 23(1)(f) and (j) thereof.   
40      In that regard, it is irrelevant that the processing of personal data is based on a provision of substantive or procedural national law, since the provisions of Article 6(3)(b) and (4) of that regulation make no distinction between those two types of provision.  
41      In the light of all the foregoing considerations, the answer to the first question is that Article 6 (3) and (4) of the GDPR must be interpreted as meaning that that provision applies, in the context of civil court proceedings, to the production as evidence of a staff register containing personal data of third parties collected principally for the purposes of tax inspection.  
   
The second question  
42      By its second question, the referring court asks, in essence, whether Articles 5 and 6 of the GDPR must be interpreted as meaning that, when assessing whether the production of a document containing personal data must be ordered in civil court proceedings, the national court is required to have regard to the interests of the data subjects concerned. If so, that court also asks whether EU law, and the GDPR in particular, lays down any specific requirements as to how that assessment is to be made.  
43      First of all, it must be pointed out that any processing of personal data must, subject to the derogations permitted in Article 23 thereof, observe the principles governing the processing of personal data and the rights of the person concerned set out, respectively, in Chapters II and III of that regulation. In particular, any processing of personal data must, first, comply with the principles set out in Article 5 of that regulation and, second, satisfy the lawfulness conditions listed in Article 6 of the same regulation (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 208 and the case-law cited).  
44      In the case at hand, the referring court notes that the relevant provisions of Chapter 38 of the RB do not expressly require, during the assessment of whether the production of a document containing personal data must be ordered, regard to be had to the interests of the persons whose personal data are at issue. According to national case-law, those provisions merely require a weighing up of the relevance of the evidence against the opposing party’s interest in not releasing the information at issue.  
45      As has been found in paragraph 39 above, since those national law provisions involve the production of a document as evidence, they are capable of falling within the scope of cases of personal data processing regarded as lawful under the provisions of Article 6(3) and (4) of the GDPR, read in combination with Article 23(1)(f) and (j) thereof. This is so because the said provisions, first, are intended to secure the proper conduct of court proceedings by ensuring that individuals are able to exercise their rights where they have a ‘justified probative interest’ and, second, are necessary and proportionate to that objective.  
46      It follows from Article 6(4) of the GDPR that such processing of personal data is lawful provided that it constitutes a necessary and proportionate measure in a democratic society and safeguards the objectives referred to in Article 23 of the GDPR which it pursues. Accordingly, in order to verify those requirements, a national court is required to have regard to the opposing interests involved when assessing whether to order the production of a document containing personal data of third parties.  
47      In that respect, it is important to stress that the result of the balancing that the national court must carry out may vary according to both the circumstances of each case and the type of proceedings at issue.  
48      So far as concerns the interests involved in civil court proceedings, the national court must, as is apparent in particular from recitals 1 and 2 of the GDPR, guarantee the protection of natural persons with regard to the processing of personal data, which is a fundamental right enshrined in Article 8(1) of the Charter and in Article 16 TFEU. That court must also guarantee the right to respect for private life, enshrined in Article 7 of the Charter, which is closely linked to the right to the protection of personal data.  
49      However, as recital 4 of the GDPR states, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced, in accordance with the principle of proportionality, against other fundamental rights, such as the right to effective judicial protection, guaranteed in Article 47 of the Charter.  
50      The production of a document containing the personal data of third parties in civil court proceedings contributes, as the Advocate General noted, in essence, in point 61 of her Opinion, to compliance with that right to effective judicial protection.  
51      In that regard, the second paragraph of Article 47 of the Charter, corresponding to Article 6(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950, its meaning and scope are, in accordance with Article 52(3) of the Charter, the same as those conferred by that convention on that Article 6(1).  
52      According to the settled case-law of the European Court of Human Rights, in view of the prominent place held in a democratic society by the right to a fair trial, it is essential that an individual have the right to present his or her case effectively before the court and enjoy equality of arms with the opposing side (see, to that effect, ECtHR, 24 June 2022,   
Zayidov v. Azerbaijan (No 2)  
, CE:ECHR:2022:0324JUD000538610, § 87 and the case-law cited). It follows, inter alia, that an individual must have the benefit of adversarial proceedings and be able to submit, at various stages of those proceedings, the arguments he or she considers relevant to his or her case (ECtHR, 21 January 1999,   
García Ruiz v. Spain  
, CE:ECHR:1999:0121JUD003054496, § 29).  
53      Therefore, in order to ensure that individuals can enjoy a right to effective judicial protection and, in particular, a right to a fair trial, within the meaning of the second paragraph of Article 47 of the Charter, the parties to civil court proceedings must be in a position to access the evidence necessary to establish to the requisite standard the merits of their complaints, which may possibly include personal data of the parties or of third parties.   
54      That being so, as has been indicated in paragraph 46 above, having regard to the interests involved forms part of the examination of the necessity and proportionality of the measure, which are provided for in Article 6(3) and (4) of the GDPR and which condition the lawfulness of the personal data processing. In that regard, account should therefore also be taken of Article 5(1) thereof, and in particular of the principle of ‘data minimisation’ set out in Article 5(1)(c), which gives expression to the principle of proportionality. According to that data minimisation principle, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 98 and the case-law cited).  
55      The national court is therefore required to determine whether the disclosure of personal data is adequate and relevant for the purpose of attaining the objective pursued by the applicable provisions of national law and whether that objective cannot be achieved by recourse to less intrusive means of proof in respect of the protection of the personal data of a large number of third parties such as, for example, the hearing of selected witnesses.   
56      In the event that the production of a document containing personal data proves to be justified, it also follows from that principle that, where only part of those data appears necessary for evidential purposes, the national court must consider taking additional data protection measures, such as the pseudonymisation, defined in Article 4(5) of the GDPR, of the names of the data subjects or any other measure intended to minimise the interference with the right to the protection of personal data resulting from the production of such a document. Such measures may include limiting public access to the file or an order addressed to the parties to whom the documents containing personal data have been disclosed not to use those data for a purpose other than the taking of evidence during the court proceedings at issue.  
57      In that regard, it should be noted that it follows from Article 4(5) of the GDPR, read in combination with recital 26 thereof, that pseudonymised personal data which could be attributed to a natural person with the use of additional information should be considered to be information on an identifiable natural person, to which the principles of data protection apply. By contrast, it follows from that recital that those principles do not apply ‘to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable’.  
58      It follows that a national court may take the view that the personal data of the parties or of third parties must be communicated to it in order to be able to balance, in full knowledge of the facts and in compliance with the principle of proportionality, the interests involved. That assessment may, depending on the case, lead it to authorise the full or partial disclosure to the opposing party of the personal data thus communicated to it, if it finds that such disclosure does not go beyond what is necessary for the purpose of guaranteeing the effective enjoyment of the rights which individuals derive from Article 47 of the Charter.  
59      In the light of all the foregoing considerations, the answer to the second question is that Articles 5 and 6 of the GDPR must be interpreted as meaning that, when assessing whether the production of a document containing personal data must be ordered, the national court is required to have regard to the interests of the data subjects concerned and to balance them according to the circumstances of each case, the type of proceeding at issue and duly taking into account the requirements arising from the principle of proportionality as well as, in particular, those resulting from the principle of data minimisation referred to in Article 5(1)(c) of that regulation.  
   
Costs  
60      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 6(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),   
must be interpreted as meaning that that provision applies, in the context of civil court proceedings, to the production as evidence of a staff register containing personal data of third parties collected principally for the purposes of tax inspection.  
2.        
Articles 5 and 6 of Regulation 2016/679  
must be interpreted as meaning that when assessing whether the production of a document containing personal data must be ordered, the national court is required to have regard to the interests of the data subjects concerned and to balance them according to the circumstances of each case, the type of proceeding at issue and duly taking into account the requirements arising from the principle of proportionality as well as, in particular, those resulting from the principle of data minimisation referred to in Article 5(1)(c) of that regulation.

ID: 0da01a04-70e4-4a3d-a80b-c6c9728106d1

Judgment of 14 Feb 2019, C-345/17 (  
Buivids  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Household exemption   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Processing   
General data protection law   
 >   
Chapter IX - Provisions relating to specific processing operations   
 >   
Processing and freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
   
JUDGMENT OF THE COURT (Second Chamber)  
14 February 2019 (\*)  
(Reference for a preliminary ruling — Processing of personal data — Directive 95/46/EC — Article 3 — Scope — Video recording of police officers carrying out procedural measures in a police station — Publication on a video website — Article 9 — Processing of personal data solely for journalistic purposes — Meaning — Freedom of expression — Protection of privacy)  
In Case C–345/17,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Augstākā tiesa (Supreme Court, Latvia), made by decision of 1 June 2017, received at the Court on 12 June 2017, in the proceedings  
Sergejs Buivids  
intervener:  
Datu valsts inspekcija,  
THE COURT (Second Chamber),  
composed of K. Lenaerts, President of the Court, acting as President of the Second Chamber, A. Prechal, C. Toader, A. Rosas (Rapporteur) and M. Ilešič, Judges,  
Advocate General: E. Sharpston,  
Registrar: M. Aleksejev, Head of Unit,  
having regard to the written procedure and further to the hearing on 21 June 2018,  
after considering the observations submitted on behalf of:  
–        Mr Buivids, by himself,  
–        the Latvian Government, by I. Kucina, G. Bambāne, E. Petrocka-Petrovska and E. Plaksins, acting as Agents,  
–        the Czech Government, by M. Smolek, J. Vláčil and O. Serdula, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by M. Russo, avvocato dello Stato,  
–        the Austrian Government, by G. Eberhard, acting as Agent,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes, M. Figueiredo and C. Vieira Guerra, acting as Agents,  
–        the Swedish Government, by A. Falk, C. Meyer-Seitz, P. Smith, H. Shev, L. Zettergren and A. Alriksson, acting as Agents,  
–        the European Commission, by D. Nardi and I. Rubene, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 27 September 2018,  
gives the following  
Judgment  
1        This request for a preliminary ruling relates to the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), and in particular of Article 9 thereof.  
2        The request has been made in proceedings between Mr Sergejs Buivids and the Datu valsts inspekcija (National Data Protection Agency, Latvia) concerning an action seeking a declaration as to the illegality of a decision of that authority, according to which Mr Buivids infringed national law by publishing a video, filmed by him, on the internet site www.youtube.com of the statement which he made in the context of administrative proceedings involving the imposition of a penalty in a station of the Latvian national police.  
   
Legal context  
   
EU law  
3        Prior to its repeal by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (OJ 2016 L 119, p. 1), Directive 95/46, which, according to Article 1 thereof, had the object of protecting the fundamental rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data, and the elimination of obstacles to the free movement of such data, stated in recitals 2, 14, 15, 17, 27 and 37:  
‘(2)      Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;  
…  
(14)      Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;  
(15)      Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;  
…  
(17)      Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;  
…  
(27)      Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; …  
…  
(37)      Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms [signed at Rome on 4 November 1950]; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, ...’  
4        Article 2 of Directive 95/46 provided:  
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or [EU] laws or regulations, the controller or the specific criteria for his nomination may be designated by national or [EU] law;  
…’  
5        Article 3 of that directive, headed ‘Scope’, provided:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of [EU] law, such as those provided for by Titles V and VI of the Treaty on European Union [in its version prior to the entry into force of the Treaty of Lisbon] and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
6        Article 7 of that directive was worded as follows:  
‘Member States shall provide that personal data may be processed only if:  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
7        Article 9 of that directive provided:  
‘Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.’  
   
Latvian law  
8        Pursuant to Article 1 of the Fizisko personu datu aizsardzības likums (Personal Data Protection Law) of 23 March 2000 (  
Latvijas Vēstnesis  
, 2000, No 123/124; ‘the Personal Data Protection Law’), the purpose of that law is to protect the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard to the processing of personal data of individuals.  
9        Pursuant to Article 2(3) the Personal Data Protection Law, the term ‘personal data’ is to be taken to mean any information concerning an identified or identifiable natural person.  
10      Under Article 2(4) of that law, the term ‘processing of personal data’ refers to any operation applied to personal data, including the collection, recording, insertion, storage, organisation, alteration, use, transfer, transmission and dissemination, blocking or deletion of data.  
11      Article 3(1) of the Personal Data Protection Law provides that that law, without prejudice to the exceptions provided for in that provision, applies to the processing of every kind of personal data and to every natural or legal person, if:  
–        the data controller is registered in Latvia;  
–        the data processing is carried out outside the borders of Latvia, in territories belonging to the latter under international agreements;  
–        in the Republic of Latvia there are facilities used for the processing of personal data, except in cases where the facilities are used only for the transmission of personal data via the territory of the Republic of Latvia.  
12      Article 3(3) of that law provides that the latter does not apply to the processing of personal data carried out by natural persons for personal or domestic and family use.  
13      Under Article 5 of the Personal Data Protection Law, save as otherwise provided, Articles 7 to 9, 11 and 21 of that law are not to apply when the personal data are processed for journalistic purposes in accordance with the Par presi un citiem masu informācijas līdzekļiem likums (Law on the press and other media) or for purposes of artistic or literary expression.  
14      Article 8(1) of the Personal Data Protection Law provides that, when collecting personal data, the data controller is required to provide the data subject with the following information, unless that person already possesses that information:  
–        the designation, or name and surname, and the address of the data controller;  
–        the intended purpose of the processing of the personal data.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
15      Mr Buivids made a video recording in a station of the Latvian national police while he was making a statement in the context of administrative proceedings which had been brought against him.  
16      Mr Buivids published the recorded video (‘the video in question’), which showed police officers going about their duties in the police station, on the internet site www.youtube.com, which is an internet site that allows users to publish, share and watch videos.  
17      After that video had been published, the National Data Protection Agency found, by decision of 30 August 2013, that Mr Buivids had infringed Article 8(1) of the Personal Data Protection Law because he had not informed the police officers, as persons concerned, in the manner laid down by that provision, of the intended purpose of the processing of personal data concerning them. It is submitted that Mr Buivids also failed to provide any information to the National Data Protection Agency as to the purpose of the recording and publication of the recorded video on an internet site such as to prove that the objective pursued was compliant with the provisions of the Personal Data Protection Law. The National Data Protection Agency therefore requested Mr Buivids to remove that video from the internet site www.youtube.com and from other websites.  
18      Mr Buivids brought an action before the administratīvā rajona tiesa (District Administrative Court, Latvia) seeking a declaration that that decision of the National Data Protection Agency was unlawful and claiming compensation for the harm which he claimed to have suffered. Mr Buivids stated in his application that he had wished, by the publication of the video in question, to bring to the attention of society something which he considered to constitute unlawful conduct on the part of the police. That court dismissed the action.  
19      By judgment of 11 November 2015, the Administratīvā apgabaltiesa (Regional Administrative Court, Latvia) dismissed the appeal brought by Mr Buivids against the decision of the administratīvā rajona tiesa (District Administrative Court).  
20      The Administratīvā apgabaltiesa (Regional Administrative Court) based its decision on the fact that, in the video in question, it is possible to see police facilities and a number of police officers performing their duties, to hear the conversation with the police officers, which was recorded whilst they were carrying out procedural matters, and to hear the voices of the police officers, Mr Buivids and the person accompanying him.  
21      Furthermore, that court held that it was not possible to determine whether Mr Buivids’ right to freedom of expression or the right to privacy of other persons had to take precedence, since Mr Buivids had not indicated his objective in publishing the video in question. Likewise, the video did not show current events relevant to society or dishonest conduct on the part of the police officers. As Mr Buivids had not recorded the video in question for journalistic purposes under the Law on the press and other media, or for purposes of artistic or literary expression, Article 5 of the Personal Data Protection Law was, in that court’s view, not applicable.  
22      The Administratīvā apgabaltiesa (Regional Administrative Court) therefore concluded that Mr Buivids had infringed Article 8(1) of the Personal Data Protection Law by making a recording of police officers carrying out their duties and by not informing those officers of the specific purpose of the processing of their personal data.  
23      Mr Buivids filed an appeal in cassation before the referring court, the Augstākā tiesa (Supreme Court, Latvia), against the judgment of the Administratīvā apgabaltiesa (Regional Administrative Court), invoking his right to freedom of expression.  
24      Mr Buivids has stated, inter alia, that the video in question shows public officials of the Latvian national police –– namely public persons in a place accessible to the public –– who, on that ground, fall outside the scope of the Personal Data Protection Law.  
25      The referring court expresses doubts, first, as to whether the act of filming police officers while they are carrying out their duties in a police station and the act of publishing that recorded video on the internet are matters which come within the scope of Directive 95/46. In that connection, although the referring court considers that Mr Buivids’ conduct does not come within the scope of the exceptions to the scope of that directive, as set out in Article 3(2) thereof, that court nevertheless emphasises that the recording at issue in the present case was made only once and that Mr Buivids filmed police officers carrying out their public duties, namely whilst they were acting as representatives of the public authorities. Referring to point 95 of the Opinion of Advocate General Bobek in the case   
Rīgas satiksme  
 (C-13/16, EU:C:2017:43), the referring court maintains that the main concern that justifies the protection of personal data is the risk involved in large-scale processing.  
26      Secondly, the referring court seeks guidance on the interpretation of the concept ‘solely for journalistic purposes’ in Article 9 of Directive 95/46, and the question of whether the facts, such as those alleged against Mr Buivids, are covered by that concept.  
27      In those circumstances, the Augstākā tiesa (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Do activities such as those at issue in the present case, that is to say, the recording, in a police station, of police officers carrying out procedural measures and publication of the video on the internet site www.youtube.com, fall within the scope of Directive 95/46?  
(2)      Must Directive 95/46 be interpreted as meaning that those activities may be regarded as the processing of personal data for journalistic purposes, within the meaning of Article 9 of Directive [95/46]?’  
   
Consideration of the questions referred  
   
The first question  
28      By its first question, the referring court asks, in essence, whether Article 3 of Directive 95/46 must be interpreted as meaning that the recording of a video of police officers in a police station, while a statement is being made, and the publication of that video on a video website, on which users can send, watch and share videos, are matters which come within the scope of that directive.  
29      It should be noted that, pursuant to Article 3(1) thereof, Directive 95/46 applies to ‘the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system’.  
30      The concept of ‘personal data’ within the meaning of that provision encompasses, according to the definition in Article 2(a) of that directive, ‘any information relating to an identified or identifiable natural person’. An identifiable person is ‘one who can be identified, directly or indirectly, in particular by reference to … one or more factors specific to his physical … identity’.  
31      According to the case-law of the Court, the image of a person recorded by a camera constitutes ‘personal data’ within the meaning of Article 2(a) of Directive 95/46 inasmuch as it makes it possible to identify the person concerned (see, to that effect, judgment of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraph 22).  
32      In the present case, it is apparent from the order for reference that it is possible to see and hear the police officers in the video in question, with the result that it must be held that those recorded images of persons constitute personal data within the meaning of Article 2(a) of Directive 95/46.  
33      As regards the concept of the ‘processing of personal data’, this is defined in Article 2(b) of Directive 95/46 as ‘any operation or set of operations which is performed upon personal data … such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction’.  
34      In the context of a video-surveillance system, the Court has held that a video recording of persons which is stored on a continuous recording device — the hard disk drive of that system — constitutes, pursuant to Article 2(b) and Article 3(1) of Directive 95/46, the automatic processing of personal data (see, to that effect, judgment of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraphs 23 and 25).  
35      At the hearing before the Court of Justice, Mr Buivids stated that he had used a digital photo camera to record the video in question. This is a video recording of persons which is stored on a continuous recording device, namely the memory of that camera. Thus, such a recording constitutes a processing of personal data by automatic means within the meaning of Article 3(1) of that directive.  
36      In that connection, the fact that such a recording was made on only one occasion has no bearing on the issue of whether that operation comes within the scope of Directive 95/46. As is apparent from the wording of Article 2(b) of that directive, read in conjunction with Article 3(1) thereof, that directive applies to ‘any operation’ which constitutes the processing of personal data within the meaning of those provisions.  
37      The Court has held that the operation of loading personal data onto an internet page must be regarded as constituting such processing (see, to that effect, judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 25, and of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 26).  
38      In that connection, the Court has also specified that placing information on an internet page entails the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet. Such operations are performed, at least in part, automatically (see, to that effect, judgment of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 26).  
39      Thus, it must be held that the act of publishing a video recording, such as the video in question, which contains personal data, on a video website on which users can send, watch and share videos, constitutes processing of those data wholly or partly by automatic means, within the meaning of Article 2(b) and Article 3(1) of Directive 95/46.  
40      Furthermore, in accordance with Article 3(2) of Directive 95/46, the latter does not apply to two types of processing of personal data. The first of these is the processing of data for the exercise of an activity which falls outside the scope of EU law, such as those provided for by Titles V and VI of the Treaty on European Union, in its version prior to the entry into force of the Treaty of Lisbon, and in any event processing operations which concern public security, defence, State security and the activities of the State in areas of criminal law. Secondly, that provision excludes the processing of personal data by a natural person in the course of a purely personal or household activity.  
41      In so far as they render inapplicable the system of protection of personal data provided for in Directive 95/46 and thus deviate from the objective underlying it, namely to ensure the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data, such as the right to respect for private and family life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’), the exceptions provided for in Article 3(2) of that directive must be interpreted strictly (see, to that effect, judgments of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraph 38, and of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 37).  
42      With regard to the main proceedings, it is apparent from the information submitted to the Court that, first, the recording and publication of the video in question cannot be regarded as a processing of personal data in the exercise of an activity which falls outside the scope of EU law, nor can it be understood as a processing operation which concerns public security, defence, State security and the activities of the State in areas of criminal law, within the meaning of the first indent of Article 3(2) of Directive 95/46. In that regard, the Court has held that the activities which are mentioned by way of example in that article are, in any event, activities of the State or of State authorities unrelated to the fields of activity of individuals (see, to that effect, judgment of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraph 36 and the case-law cited).  
43      Secondly, since Mr Buivids published the video in question on a video website on which users can send, watch and share videos, without restricting access to that video, thereby permitting access to personal data to an indefinite number of people, the processing of personal data at issue in the main proceedings does not come within the context of purely personal or household activities (see, by analogy, judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 47; of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 44; of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraphs 31 and 33; and of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 42).  
44      Moreover, the act of recording a video of police officers in the performance of their duties is not capable of excluding such a type of processing of personal data from coming within the scope of Directive 95/46.  
45      As the Advocate General observes in point 29 of her Opinion, that directive contains no express exception which excludes the processing of personal data of public officials from its scope.  
46      Furthermore, it is apparent from the Court’s case-law that the fact that information is provided as part of a professional activity does not mean that it cannot be characterised as ‘personal data’ (see, to that effect, judgment of 16 July 2015,   
ClientEarth and PAN Europe   
v  
 EFSA  
, C-615/13 P, EU:C:2015:489, paragraph 30 and the case-law cited).  
47      In the light of the foregoing, the answer to the first question is that Article 3 of Directive 95/46 must be interpreted as meaning that the recording of a video of police officers in a police station, while a statement is being made, and the publication of that video on a video website, on which users can send, watch and share videos, are matters which come within the scope of that directive.  
   
The second question  
48      By its second question, the referring court asks, in essence, whether Article 9 of Directive 95/46 must be interpreted as meaning that factual circumstances such as those of the main proceedings, that is to say, the recording of a video of police officers in a police station, while a statement is being made, and the publication of that recorded video on a video website, on which users can send, watch and share videos, constitute processing of personal data for journalistic purposes, within the meaning of that provision.  
49      It must be observed, as a preliminary point, that, according to settled case-law of the Court, the provisions of a directive must be interpreted in the light of the aims pursued by the directive and the system which it establishes (judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 51 and the case-law cited).  
50      In that regard, it is apparent from Article 1 of Directive 95/46 that its objective is that the Member States should, while permitting the free flow of personal data, protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy, with respect to the processing of personal data. That objective cannot, however, be pursued without having regard to the fact that those fundamental rights must, to some degree, be reconciled with the fundamental right to freedom of expression. Recital 37 of Directive 95/46 makes it clear that Article 9 seeks to reconcile two fundamental rights: the protection of privacy and freedom of expression. This is a task for the Member States (see, to that effect, judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraphs 52 to 54).  
51      The Court has already held that, in order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly (see, to that effect, judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 56).  
52      Thus, it is apparent from the legislative history of Directive 95/46 that the exemptions and derogations provided for in Article 9 of that directive apply not only to media undertakings but also to every person engaged in journalism (see, to that effect, judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 58).  
53      It follows from the Court’s case-law that ‘journalistic activities’ are those which have as their purpose the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them (see, to that effect, judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 61).  
54      Although it is for the referring court to determine whether, in the present case, the processing of personal data by Mr Buivids serves that objective, the fact remains that the Court may provide the referring court with the elements of interpretation which are necessary for its assessment.  
55      Thus, having regard to the case-law of the Court cited in paragraphs 52 and 53 of the present judgment, the fact that Mr Buivids is not a professional journalist does not appear to be capable of excluding the possibility that the recording of the video in question and its publication on a video website, on which users can send, watch and share videos, may come within the scope of that provision.  
56      In particular, the fact that Mr Buivids uploaded the recorded video online on such an internet site, in this case www.youtube.com, cannot in itself preclude the classification of that processing of personal data as having been carried out ‘solely for journalistic purposes’, within the meaning of Article 9 of Directive 95/46.  
57      Account must be taken of the evolution and proliferation of methods of communication and the dissemination of information. Thus, the Court has already held that the medium which is used to transmit the processed data, whether it be classic in nature, such as paper or radio waves, or electronic, such as the internet, is not determinative as to whether an activity is undertaken ‘solely for journalistic purposes’ (see, to that effect, judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 60).  
58      That said, as observed, in essence, by the Advocate General in point 55 of her Opinion, the view cannot be taken that all information published on the internet, involving personal data, comes under the concept of ‘journalistic activities’ and thus benefits from the exemptions or derogations provided for in Article 9 of Directive 95/46.  
59      In the present case, it is for the referring court to determine whether it appears from the video in question that the sole purpose of the recording and publication of the video was the disclosure to the public of information, opinions or ideas (see, to that effect, judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 62).  
60      To that end, the referring court may, in particular, take into consideration the fact that, according to Mr Buivids, the video in question was published on an internet site to draw to the attention of society alleged police malpractice which, he claims, occurred while he was making his statement.  
61      It should be noted, however, that the establishment of such malpractice is not a condition for the applicability of Article 9 of Directive 95/46.  
62      By contrast, should it transpire that the recording and publication of the video were not intended solely to disclose information, opinions or ideas to the public, it cannot be held that the processing of the personal data at issue was carried out ‘solely for journalistic purposes’.  
63      It should be noted that the exemptions and derogations in Article 9 of Directive 95/46 must be applied only where they are necessary in order to reconcile two fundamental rights, namely the right to privacy and the right to freedom of expression (see, to that effect, judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 55).  
64      Thus, in order to achieve a balance between those two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in Chapters II, IV and VI of Directive 95/46 must apply only in so far as is strictly necessary (see, to that effect, judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 56).  
65      It should be noted that Article 7 of the Charter, concerning the right to respect for private and family life, contains rights which correspond to those guaranteed by Article 8(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950, (‘the ECHR’) and that, in accordance with Article 52(3) of the Charter, Article 7 thereof is thus to be given the same meaning and the same scope as Article 8(1) ECHR, as interpreted by the case-law of the European Court of Human Rights (judgment of 17 December 2015,   
WebMindLicenses  
, C-419/14, EU:C:2015:832, paragraph 70). The same is true of Article 11 of the Charter and Article 10 ECHR (see, to that effect, judgment of 4 May 2016,   
Philip Morris Brands and Others  
, C-547/14, EU:C:2016:325, paragraph 147).  
66      In that connection, it is apparent from that case-law that, in order to balance the right to privacy and the right to freedom of expression, the European Court of Human Rights has laid down a number of relevant criteria which must be taken into account, inter alia, contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, and the manner and circumstances in which the information was obtained and its veracity (see, to that effect, judgment of the ECtHR of 27 June 2017,   
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland  
, CE:ECHR:2017:0627JUD000093113, § 165) Similarly, the possibility for the controller to adopt measures to mitigate the extent of the interference with the right to privacy must be taken into account.  
67      In the present case, it is apparent from the documents submitted to the Court that it cannot be ruled out that the recording and publication of the video in question, which took place without the persons concerned being informed of the recording and its purposes, constitutes an interference with the fundamental right to privacy of those persons, namely the police officers featured in that video.  
68      If it should transpire that the sole objective of the recording and publication of the video in question was the disclosure to the public of information, opinions or ideas, it is for the referring court to determine whether the exemptions or derogations provided for in Article 9 of Directive 95/46 are necessary in order to reconcile the right to privacy with the rules governing freedom of expression, and whether those exemptions and derogations are applied only in so far as is strictly necessary.  
69      In the light of the foregoing considerations, the answer to the second question is that Article 9 of Directive 95/46 must be interpreted as meaning that factual circumstances such as those of the case in the main proceedings, that is to say, the video recording of police officers in a police station, while a statement is being made, and the publication of that recorded video on a video website, on which users can send, watch and share videos, may constitute a processing of personal data solely for journalistic purposes, within the meaning of that provision, in so far as it is apparent from that video that the sole object of that recording and publication thereof is the disclosure of information, opinions or ideas to the public, this being a matter which it is for the referring court to determine.  
   
Costs  
70      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
1.        
Article 3 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the recording of a video of police officers in a police station, while a statement is being made, and the publication of that video on a video website, on which users can send, watch and share videos, are matters which come within the scope of that directive.  
2.        
Article 9 of Directive 95/46 must be interpreted as meaning that factual circumstances such as those of the case in the main proceedings, that is to say, the video recording of police officers in a police station, while a statement is being made, and the publication of that recorded video on a video website, on which users can send, watch and share videos, may constitute a processing of personal data solely for journalistic purposes, within the meaning of that provision, in so far as it is apparent from that video that the sole object of that recording and publication thereof is the disclosure of information, opinions or ideas to the public, this being a matter which it is for the referring court to determine.

ID: 10ae8872-62e3-4621-9e1e-b46ad9793f4f

Judgment of 1 Oct 2019, C-673/17 (  
Planet49  
)  
E-privacy Directive   
 >   
Cookies   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Consent   
E-privacy Directive   
 >   
Cookies   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Information to be provided in case of direct collection   
   
JUDGMENT OF THE COURT (Grand Chamber)  
1 October 2019(\*)  
(Reference for a preliminary ruling — Directive 95/46/EC — Directive 2002/58/EC — Regulation (EU) 2016/679 — Processing of personal data and protection of privacy in the electronic communications sector — Cookies — Concept of consent of the data subject — Declaration of consent by means of a pre-ticked checkbox)  
In Case C-673/17,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 5 October 2017, received at the Court on 30 November 2017, in the proceedings  
Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV  
v  
Planet49 GmbH,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, J.-C. Bonichot, M. Vilaras, T. von Danwitz, C. Toader, F. Biltgen, K. Jürimäe and C. Lycourgos, Presidents of Chambers, A. Rosas (Rapporteur), L. Bay Larsen, M. Safjan and S. Rodin, Judges,  
Advocate General: M. Szpunar,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 13 November 2018,  
after considering the observations submitted on behalf of:  
–        the Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV, by P. Wassermann, Rechtsanwalt,  
–        Planet49 GmbH, by M. Jaschinski, J. Viniol and T. Petersen, Rechtsanwälte,  
–        the German Government, by J. Möller, acting as Agent,  
–        the Italian Government, by G. Palmieri, acting as Agent, and F. De Luca, avvocato dello Stato,  
–        the Portuguese Government, by L. Inez Fernandes, M. Figueiredo, L. Medeiros and C. Guerra, acting as Agents,  
–        the European Commission, by G. Braun, H. Kranenborg and P. Costa de Oliveira, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 21 March 2019,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2(f) and of Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), read in conjunction with Article 2(h) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), and of Article 6(1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation) (OJ 2016 L 119, p. 1).  
2        The request has been made in proceedings between the Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV (Federal Union of Consumer Organisations and Associations — Federation of Consumer Organisations, Germany) (‘the Federation’) and Planet49 GmbH, an online gaming company, concerning the consent of participants in a promotional lottery organised by that company to the transfer of their personal data to the company’s sponsors and partners, to the storage of information and to the access to information stored in the terminal equipment of those users.  
   
Legal context  
   
EU law  
   
Directive 95/46  
3        Article 1 of Directive 95/46 provides:  
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
4        Article 2 of the directive provides:  
‘For the purposes of this Directive:  
(a)      “Personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
...  
(h)      “the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.’  
5        Article 7 of that directive states:  
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent  
...’  
6        Under Article 10 of that directive:  
‘Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:  
(a)      the identity of the controller and of his representative, if any;  
(b)      the purposes of the processing operation for which the data are intended;  
(c)      any further information such as  
–        the recipients or categories of recipients of the data,  
–        whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,  
–        the existence of the right of access to and the right to rectify the data concerning him or her,  
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.’  
   
Directive 2002/58  
7        Recitals 17 and 24 of Directive 2002/58 state:  
‘(17)      For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject’s consent as defined and further specified in Directive [95/46]. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an internet website.  
...  
(24)      Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms [signed in Rome on 4 November 1950]. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user’s terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.’  
8        Article 1 of Directive 2002/58 provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the [European Union].  
2.      The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. ...’  
9        Article 2 of the directive provides:  
‘Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [OJ 2002, L 108, p. 33] shall apply.  
The following definitions shall also apply:  
(a)      “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;  
...  
(f)      “consent” by a user or subscriber corresponds to the data subject’s consent in Directive [95/46];  
...’  
10      Article 5(3) of the directive provides:  
‘Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
   
Regulation 2016/679  
11      Recital 32 of Regulation 2016/679 states:  
‘Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.’  
12      Article 4 of that regulation provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;   
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
...  
(11)      “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;  
...’  
13      Article 6 of the regulation provides:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:   
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
...’  
14      Article 7(4) of the regulation provides:  
‘When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.’  
15      Under Article 13(1) and (2) of Regulation 2016/679:  
‘1.      Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:   
...  
(e)      the recipients or categories of recipients of the personal data ...  
...  
2.      In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:   
(a)      the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;  
...’  
16      Article 94 of that regulation provides:  
‘1.      Directive [95/46] is repealed with effect from 25 May 2018.  
2.      References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.’  
   
German law  
17      According to the first sentence of Paragraph 307(1) of the Bürgerliches Gesetzbuch (German Civil Code; ‘the BGB’), ‘provisions in standard business terms are ineffective if, contrary to the requirement of good faith, they unreasonably disadvantage the other party to the contract with the user’.  
18      Paragraph 307(2)(1) of the BGB provides that, in cases of doubt, ‘an unreasonable disadvantage is to be assumed if a provision is not reconcilable with essential underlying ideas of the statutory provision which is deviated from’.  
19      Paragraph 12 of the Telemediengesetz (Law on telemedia) of 26 February 2007 (BGBl. 2007 I, p. 179) in the version in force at the material time in the main proceedings (‘the TMG’) provides:  
‘(1)      A service provider may collect and use personal data to make telemedia available only in so far as this Law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.  
(2)      Where personal data have been supplied in order for telemedia to be made available, a service provider may use them for other purposes only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.  
(3)      Except as otherwise provided, the provisions concerning the protection of personal data which are applicable in the case in question shall apply even if the data are not processed automatically.’  
20      According to Paragraph 13(1) of the TMG, at the beginning of the act of use, the service provider must inform the user about the nature, scope and purposes of the collection and use of personal data in a generally understandable form, to the extent that such information has not already been provided. In the case of an automated process allowing subsequent identification of the user and which prepares the collection or use of personal data, the user shall be informed at the beginning of this process.  
21      According to Paragraph 15(3) of the TMG, the service provider may, for the purposes of advertising, market research or designing the telemedia in order to meet requirements, create use profiles employing pseudonyms if the user does not object to this after being informed of his right to object.  
22      Under Paragraph 3(1) of the Bundesdatenschutzgesetz (Federal Law on data protection) of 20 December 1990 (BGBl. 1990 I, p. 2954), in the version in force at the material time in the main proceedings (‘the BDSG’), ‘personal data means details of personal or material circumstances of a determined or determinable natural person (data subject)’.  
23      According to the definition in Paragraph 3(3) of the BDSG, collection means the acquisition of data about the data subject.  
24      The first sentence of Paragraph 4a(1) of the BDSG, which transposes Article 2(h) of Directive 95/46, specifies that consent is effective only if it is based on a free decision by the data subject.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
25      On 24 September 2013, Planet49 organised a promotional lottery on the website www.dein-macbook.de.  
26      Internet users wishing to take part in that lottery were required to enter their postcodes, which redirected them to a web page where they were required to enter their names and addresses. Beneath the input fields for the address were two bodies of explanatory text accompanied by checkboxes. The first body of text with a checkbox without a preselected tick (‘the first checkbox’) read:  
‘I agree to certain   
sponsors and cooperation partners  
 providing me with information by post or by telephone or by email/SMS about offers from their   
respective commercial sectors  
. I can determine these myself here; otherwise, the selection is made by the organiser. I can revoke this consent at any time.   
Further information about this can be found here  
.’  
27      The second set of text with a checkbox containing a preselected tick (‘the second checkbox’) read:  
‘I agree to the web analytics service Remintrex being used for me. This has the consequence that, following registration for the lottery, the lottery organiser, [Planet49], sets cookies, which enables Planet49 to evaluate my surfing and use behaviour on websites of advertising partners and thus enables advertising by Remintrex that is based on my interests. I can delete the cookies at any time. You can read more about this   
here  
.’  
28      Participation in the lottery was possible only if at least the first checkbox was ticked.  
29      The hyperlink associated with the words ‘sponsors and cooperation partners’ and ‘here’ next to the first checkbox opened a list of 57 companies, their addresses, the commercial sector to be advertised and the method of communication used for the advertising (email, post or telephone). The underlined word ‘Unsubscribe’ was contained after the name of each company. The following statement preceded the list:  
‘By clicking on the “Unsubscribe” link, I am deciding that no advertising consent is permitted to be granted to the partner/sponsor in question. If I have not unsubscribed from any or a sufficient number of partners/sponsors, Planet49 will choose partners/sponsors for me at its discretion (maximum number: 30 partners/sponsors).’  
30      When the hyperlink associated with the word ‘here’ next to the second checkbox was clicked on, the following information was displayed:  
‘The cookies named ceng\_cache, ceng\_etag, ceng\_png and gcr are small files which are stored in an assigned manner on your hard disk by the browser you use and by means of which certain information is supplied which enables more user-friendly and effective advertising. The cookies contain a specific randomly generated number (ID), which is at the same time assigned to your registration data. If you then visit the website of an advertising partner which is registered for Remintrex (to find out whether a registration exists, please consult the advertising partner’s data protection declaration), Remintrex automatically records, by virtue of an iFrame which is integrated there, that you (or the user with the stored ID) have visited the site, which product you have shown interest in and whether a transaction was entered into.  
Subsequently, [Planet49] can arrange, on the basis of the advertising consent given during registration for the lottery, for advertising emails to be sent to you which take account of your interests demonstrated on the advertising partner’s website. After revoking the advertising consent, you will of course not receive any more email advertising.   
The information communicated by these cookies is used exclusively for the purposes of advertising in which products of the advertising partner are presented. The information is collected, stored and used separately for each advertising partner. User profiles involving multiple advertising partners will not be created under any circumstances. The individual advertising partners do not receive any personal data.  
If you have no further interest in using the cookies, you can delete them via your browser at any time. You can find a guide in your browser’s [“help”] function.   
No programs can be run or viruses transmitted by means of the cookies.  
You of course have the option to revoke this consent at any time. You can send the revocation in writing to [Planet49] [address]. However, an email to our customer services department [email address] will also suffice.’  
31      According to the order for reference, cookies are text files which the provider of a website stores on the website user’s computer which that website provider can access again when the user visits the website on a further occasion, in order to facilitate navigation on the internet or transactions, or to access information about user behaviour.  
32      In an unanswered letter before action, the Federation, which is registered on the list of entities entitled to bring court proceedings pursuant to Paragraph 4 of the Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz — UKlaG) (Law relating to injunctions in the case of breaches of consumer law and of other laws, ‘the UKlaG’) of 26 November 2001 (BGBl. 2001 I, p. 3138), asserted that the declarations of consent requested by Planet49 through the first and second checkboxes did not satisfy the requirements of Paragraph 307 of the BGB, read in conjunction with Paragraph 7(2)(2) of the Gesetz gegen den unlauteren Wettbewerb (Law against Unfair Competition) of 3 July 2004 (BGBl. 2004 I, p. 1414), in the version in force at the material time in the main proceedings, and Paragraph 12 et seq. of the TMG.  
33      The Federation brought an action before the Landgericht Frankfurt am Main (Regional Court, Frankfurt am Main, Germany) for an injunction, in substance, requiring Planet49 to cease using such declarations and to pay it EUR 214 plus interest from 15 March 2014.  
34      The Landgericht Frankfurt am Main (Regional Court, Frankfurt am Main) upheld the action in part.   
35      Following an appeal on points of fact and law brought by Planet49 before the Oberlandesgericht Frankfurt am Main (Higher Regional Court, Frankfurt am Main, Germany), that court held that the Federation’s plea for an injunction ordering Planet49 to refrain from including the statement set out in paragraph 27 above, the checkbox for which was pre-checked, in consumer lottery agreements, was unfounded in that, first, the user would realise that he or she could deselect the tick in that checkbox and, second, the text was set out with sufficient clarity from a typographical point of view and provided information about the manner of the use of cookies without it being necessary to disclose the identity of third parties able to access the information collected.  
36      The Bundesgerichtshof (Federal Court of Justice, Germany), before which the Federation brought an appeal on a point of law (  
Revision  
), considers that the success of the appeal in the main proceedings turns on the interpretation of Article 5(3) and Article 2(f) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 6(1)(a) of Regulation 2016/679.  
37      Harbouring doubts as to the validity, in the light of those provisions, of the consent obtained by Planet49 from internet users of the website www.dein-macbook.de by means of the second checkbox and as to the extent of the information obligation provided for in Article 5(3) of Directive 2002/58, the Bundesgerichtshof (Federal Court of Justice) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)(a)      Does it constitute a valid consent within the meaning of Article 5(3) and Article 2(f) of Directive [2002/58], read in conjunction with Article 2(h) of Directive [95/46], if the storage of information, or access to information already stored in the user’s terminal equipment, is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent?   
(b)      For the purposes of the application of Article 5(3) and of Article 2(f) of Directive [2002/58] read in conjunction with Article 2(h) of Directive [95/46], does it make a difference whether the information stored or accessed constitutes personal data?  
(c)      In the circumstances referred to in Question 1(a), does a valid consent within the meaning of Article 6(1)(a) of Regulation [2016/679] exist?  
(2)      What information does the service provider have to give within the scope of the provision of clear and comprehensive information to the user that has to be undertaken in accordance with Article 5(3) of Directive [2002/58]? Does this include the duration of the operation of the cookies and the question of whether third parties are given access to the cookies?’  
   
Consideration of the questions referred  
   
Preliminary observations  
38      As a preliminary matter, it is appropriate to consider the applicability of Directive 95/46 and Regulation 2016/679 to the facts at issue in the main proceedings.  
39      Under Article 94(1) of Regulation 2016/679, Directive 95/46 was repealed and replaced by that regulation with effect from 25 May 2018.  
40      Indeed, that date is more recent than the date of the last hearing before the referring court, which took place on 14 July 2017, and more recent than the date on which the request for a preliminary ruling was referred by the national court.  
41      However, the referring court stated that, in view of the entry into force, on 25 May 2018, of Regulation 2016/679, to which part of the first question refers, it was likely that that regulation would need to be taken into account when disposing of the case in the main proceedings. In addition, as the German Government stated at the hearing before the Court, it is not inconceivable that, in so far as the proceedings brought by the Federation seek an order that Planet49 refrain from future action, Regulation 2016/679 would be applicable   
ratione temporis  
 to the case in the main proceedings according to the national case-law regarding the relevant legal position on injunctions, which is for the referring court to ascertain (see, as regards an action for a declaratory judgment, judgment of 16 January 2019,   
Deutsche Post  
, C-496/17, EU:C:2019:26, paragraph 38).  
42      In those circumstances, and in the light of the fact that, under Article 94(2) of Regulation 2016/679, the references to Directive 95/46 in Directive 2002/58 are to be construed as references to that regulation, it is not inconceivable, in the present case, that Directive 2002/58 applies both to Directive 95/46 and Regulation 2016/679, according to the nature of the Federation’s pleas and the relevant time.  
43      The questions referred must therefore be answered having regard to both Directive 95/46 and Regulation 2016/679.  
   
Question 1(a) and (c)  
44      By Question 1(a) and (c), the referring court asks, in essence, whether Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 6(1)(a) of Regulation 2016/679, must be interpreted as meaning that the consent referred to in those provisions is validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user’s terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.  
45      As a preliminary matter, it is important to note that, according to the order for reference, the cookies likely to be placed on the terminal equipment of a user participating in the promotional lottery organised by Planet49 contain a number which is assigned to the registration data of that user, who must enter his or her name and address in the registration form for the lottery. The referring court adds that, by linking that number with that data, a connection between a person to the data stored by the cookies arises if the user uses the internet, such that the collection of that data by means of cookies is a form of processing of personal data. Those statements were confirmed by Planet49, which noted in its written observations that the consent to which the second checkbox refers is intended to authorise the collection and processing of personal data, not anonymous data.  
46      On the basis of those explanations, it should be noted that, in accordance with Article 5(3) of Directive 2002/58, Member States are to ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a user is only allowed on condition that the user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46, inter alia, about the purposes of the processing.  
47      In that regard, it should be noted that, the need for a uniform application of EU law and the principle of equality require that the wording of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union (judgments of 26 March 2019,   
SM (Child placed under Algerian kafala)  
, C-129/18, EU:C:2019:248, paragraph 50, and of 11 April 2019,   
Tarola  
, C-483/17, EU:C:2019:309, paragraph 36).  
48      In addition, according to settled case-law of the Court, the interpretation of a provision of EU law requires that account be taken not only of its wording and the objectives it pursues, but also of its legislative context and the provisions of EU law as a whole. The origins of a provision of EU law may also provide information relevant to its interpretation (judgment of 10 December 2018,   
Wightman and Others  
, C-621/18, EU:C:2018:999, paragraph 47 and the case-law cited).  
49      As regards the wording of Article 5(3) of Directive 2002/58, it should be made clear that, although that provision states expressly that the user must have ‘given his or her consent’ to the storage of and access to cookies on his or her terminal equipment, that provision does not, by contrast, indicate the way in which that consent must be given. The wording ‘given his or her consent’ does, however, lend itself to a literal interpretation according to which action is required on the part of the user in order to give his or her consent. In that regard, it is clear from recital 17 of Directive 2002/58 that, for the purposes of that directive, a user’s consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including ‘by ticking a box when visiting an internet website’.  
50      As regards the legislative context of which Article 5(3) of Directive 2002/58 forms a part, Article 2(f) of that directive, which defines ‘consent’, for the purposes thereof, refers, in that regard, to the ‘data subject’s consent’ set out in Directive 95/46. Recital 17 of Directive 2002/58 states that, for the purposes of that directive, consent of a user should have the same meaning as the data subject’s consent as defined and further specified in Directive 95/46.   
51      Article 2(h) of Directive 95/46 defines ‘the data subject’s consent’ as being ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’.   
52      Thus, as the Advocate General stated in point 60 of his Opinion, the requirement of an ‘indication’ of the data subject’s wishes clearly points to active, rather than passive, behaviour. However, consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of a website user.   
53      That interpretation is borne out by Article 7 of Directive 95/46, which sets out an exhaustive list of cases in which the processing of personal data can be regarded as lawful (see, to that effect, judgments of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 30, and of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 57).  
54      In particular, Article 7(a) of Directive 95/46 provides that the data subject’s consent may make such processing lawful provided that the data subject has given his or her consent ‘unambiguously’. Only active behaviour on the part of the data subject with a view to giving his or her consent may fulfil that requirement.  
55      In that regard, it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not deselecting a pre-ticked checkbox nor, in any event, whether that consent had been informed. It is not inconceivable that a user would not have read the information accompanying the preselected checkbox, or even would not have noticed that checkbox, before continuing with his or her activity on the website visited.  
56      Lastly, as regards the origins of Article 5(3) of Directive 2002/58, the initial wording of that provision provided only for the requirement that the user had the ‘right to refuse’ the storage of cookies, after having received, pursuant to Directive 95/46, clear and comprehensive information, inter alia, regarding the purpose of the data processing. Directive 2009/136 introduced a substantive amendment to the wording of that provision, by replacing that wording with ‘given his or her consent’. The legislative origins of Article 5(3) of Directive 2002/58 thus seem to indicate that henceforth user consent may no longer be presumed but must be the result of active behaviour on the part of the user.  
57      As regards the foregoing, the consent referred to in Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46, is therefore not validly constituted if the storage of information, or access to information already stored in an website user’s terminal equipment, is permitted by way of a checkbox pre-ticked by the service provider which the user must deselect to refuse his or her consent.  
58      It should be added that the indication of the data subject’s wishes referred to in Article 2(h) of Directive 95/46 must, inter alia, be ‘specific’ in the sense that it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject’s wishes for other purposes.  
59      In the present case, contrary to what Planet49 claims, the fact that a user selects the button to participate in the promotional lottery organised by that company cannot therefore be sufficient for it to be concluded that the user validly gave his or her consent to the storage of cookies.  
60      A fortiori, the preceding interpretation applies in the light of Regulation 2016/679.  
61      As the Advocate General stated, in essence, in point 70 of his Opinion, the wording of Article 4(11) of Regulation 2016/679, which defines the ‘data subject’s consent’ for the purposes of that regulation and, in particular, of Article 6(1)(a) thereof, to which Question 1(c) refers, appears even more stringent than that of Article 2(h) of Directive 95/46 in that it requires a ‘freely given, specific, informed and unambiguous’ indication of the data subject’s wishes in the form of a statement or of ‘clear affirmative action’ signifying agreement to the processing of the personal data relating to him or her.  
62      Active consent is thus now expressly laid down in Regulation 2016/679. It should be noted in that regard that, according to recital 32 thereof, giving consent could include ticking a box when visiting an internet website. On the other hand, that recital expressly precludes ‘silence, pre-ticked boxes or inactivity’ from constituting consent.  
63      It follows that the consent referred to in Article 2(f) and in Article 5(3) of Directive 2002/58, read in conjunction with Article 4(11) and Article 6(1)(a) of Regulation 2016/679, is not validly constituted if the storage of information, or access to information already stored in the website user’s terminal equipment, is permitted by way of a pre-ticked checkbox which the user must deselect to refuse his or her consent.  
64      Lastly, it should be noted that the referring court has not referred to the Court the question whether it is compatible with the requirement that consent be ‘freely given’, within the meaning of Article 2(h) of Directive 95/46 and of Article 4(11) and Article 7(4) of Regulation 2016/679, for a user’s consent to the processing of his personal data for advertising purposes to be a prerequisite to that user’s participation in a promotional lottery, as appears to be the case in the main proceedings, according to the order for reference, at least as far as concerns the first checkbox. In those circumstances, it is not appropriate for the Court to consider that question.  
65      In the light of the foregoing considerations, the answer to Question 1(a) and (c) is that Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679, must be interpreted as meaning that the consent referred to in those provisions is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user’s terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.  
   
Question 1(b)  
66      By Question 1(b), the referring court wishes to know, in essence, whether Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 6(1)(a) of Regulation 2016/679, must be interpreted differently according to whether or not the information stored or accessed on a website user’s terminal equipment is personal data within the meaning of Directive 95/46 and Regulation 2016/679.  
67      As stated in paragraph 45 above, according to the order for reference, the storage of cookies at issue in the main proceedings amounts to a processing of personal data.  
68      That being the case, the Court notes, in any event, that Article 5(3) of Directive 2002/58 refers to ‘the storing of information’ and ‘the gaining of access to information already stored’, without characterising that information or specifying that it must be personal data.  
69      As the Advocate General stated in point 107 of his Opinion, that provision aims to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data.  
70      That interpretation is borne out by recital 24 of Directive 2002/58, according to which any information stored in the terminal equipment of users of electronic communications networks are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. That protection applies to any information stored in such terminal equipment, regardless of whether or not it is personal data, and is intended, in particular, as is clear from that recital, to protect users from the risk that hidden identifiers and other similar devices enter those users’ terminal equipment without their knowledge.  
71      In the light of the foregoing considerations, the answer to Question 1(b) is that Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679, are not to be interpreted differently according to whether or not the information stored or accessed on a website user’s terminal equipment is personal data within the meaning of Directive 95/46 and Regulation 2016/679.  
   
Question 2  
72      By Question 2, the referring court asks, in essence, whether Article 5(3) of Directive 2002/58 must be interpreted as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.  
73      As has already been made clear in paragraph 46 above, Article 5(3) of Directive 2002/58 requires that the user concerned has given his or her consent, having been provided with clear and comprehensive information, ‘in accordance with Directive [95/46]’, inter alia, about the purposes of the processing.  
74      As the Advocate General stated in point 115 of his Opinion, clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed. It must be clearly comprehensible and sufficiently detailed so as to enable the user to comprehend the functioning of the cookies employed.  
75      In a situation such as that at issue in the main proceedings, in which, according to the file before the Court, cookies aim to collect information for advertising purposes relating to the products of partners of the organiser of the promotional lottery, the duration of the operation of the cookies and whether or not third parties may have access to those cookies form part of the clear and comprehensive information which must be provided to the user in accordance with Article 5(3) of Directive 2002/58.   
76      In that regard, it should be made clear that Article 10 of Directive 95/46, to which Article 5(3) of Directive 2002/58 and Article 13 of Regulation 2016/679 refer, lists the information with which the controller must provide a data subject from whom data relating to himself are collected.   
77      That information includes, inter alia, under Article 10 of Directive 95/46, in addition to the identity of the controller and the purposes of the processing for which the data are intended, any further information such as the recipients or categories of recipients of the data in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.  
78      Although the duration of the processing of the data is not included as part of that information, it is, however, clear from the words ‘at least’ in Article 10 of Directive 95/46 that that information is not listed exhaustively. Information on the duration of the operation of cookies must be regarded as meeting the requirement of fair data processing provided for in that article in that, in a situation such as that at issue in the main proceedings, a long, or even unlimited, duration means collecting a large amount of information on users’ surfing behaviour and how often they may visit the websites of the organiser of the promotional lottery’s advertising partners.  
79      That interpretation is borne out by Article 13(2)(a) of Regulation 2016/679, which provides that the controller must, in order to ensure fair and transparent processing, provide the data subject with information relating, inter alia, to the period for which the personal data will be stored, or if that is not possible, to the criteria used to determine that period.  
80      As to whether or not third parties may have access to cookies, that is information included within the information referred to in Article 10(c) of Directive 95/46 and in Article 13(1)(e) of Regulation 2016/679, since those provisions expressly refer to the recipients or categories of recipients of the data.  
81      In the light of the foregoing considerations, the answer to Question 2 is that Article 5(3) of Directive 2002/58 must be interpreted as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.  
   
Costs  
82      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 2(f) and of Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in conjunction with Article 2(h) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Article 4(11) and Article 6(1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), must be interpreted as meaning that the consent referred to in those provisions is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user’s terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.  
2.        
Article 2(f) and Article 5(3) of Directive 2002/58, as amended by Directive 2009/136, read in conjunction with Article 2(h) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679, are not to be interpreted differently according to whether or not the information stored or accessed on a website user’s terminal equipment is personal data within the meaning of Directive 95/46 and Regulation 2016/679.  
3.        
Article 5(3) of Directive 2002/58, as amended by Directive 2009/136, must be interpreted as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

ID: 14076c15-b638-4329-8f4a-cc38c9f4e66d

of 16 Jul 2020, C-311/18 (  
Facebook Ireland and Schrems  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
General data protection law   
 >   
Chapter V - International data transfer   
 >   
General principle for transfers   
General data protection law   
 >   
Chapter V - International data transfer   
 >   
Appropriate safeguards - EU Model Clauses   
General data protection law   
 >   
Chapter V - International data transfer   
 >   
Adequacy decision   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Powers   
General data protection law   
 >   
Chapter V - International data transfer   
 >   
Adequacy decision   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
General data protection law   
 >   
Chapter V - International data transfer   
 >   
Appropriate safeguards - EU Model Clauses   
General data protection law   
 >   
Chapter V - International data transfer   
 >   
Adequacy decision   
   
JUDGMENT OF THE COURT (Grand Chamber)  
16 July 2020 (\*)  
(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Regulation (EU) 2016/679 — Article 2(2) — Scope — Transfers of personal data to third countries for commercial purposes — Article 45 — Commission adequacy decision — Article 46 — Transfers subject to appropriate safeguards — Article 58 — Powers of the supervisory authorities — Processing of the data transferred by the public authorities of a third country for national security purposes — Assessment of the adequacy of the level of protection in the third country — Decision 2010/87/EU — Protective standard clauses on the transfer of personal data to third countries — Suitable safeguards provided by the data controller — Validity — Implementing Decision (EU) 2016/1250 — Adequacy of the protection provided by the EU-US Privacy Shield — Validity — Complaint by a natural person whose data was transferred from the European Union to the United States)  
In Case C-311/18,  
REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 4 May 2018, received at the Court on 9 May 2018, in the proceedings  
Data Protection Commissioner  
v  
Facebook Ireland Ltd,  
Maximillian Schrems,  
intervening parties:  
The United States of America,  
Electronic Privacy Information Centre,  
BSA Business Software Alliance   
Inc.  
,  
Digitaleurope,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P.G. Xuereb, L.S. Rossi and I. Jarukaitis, Presidents of Chambers, M. Ilešič, T. von Danwitz (Rapporteur), and D. Šváby, Judges,  
Advocate General: H. Saugmandsgaard Øe,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 9 July 2019,  
after considering the observations submitted on behalf of:  
–        the Data Protection Commissioner, by D. Young, Solicitor, B. Murray and M. Collins, Senior Counsel, and C. Donnelly, Barrister-at-Law,  
–        Facebook Ireland Ltd, by P. Gallagher and N. Hyland, Senior Counsel, A. Mulligan and F. Kieran, Barristers-at-Law, and P. Nolan, C. Monaghan, C. O’Neill and R. Woulfe, Solicitors,  
–        Mr Schrems, by H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty and S. O’Sullivan, Senior Counsel, and G. Rudden, Solicitor,  
–        the United States of America, by E. Barrington, Senior Counsel, S. Kingston, Barrister-at-Law, S. Barton and B. Walsh, Solicitors,  
–        the Electronic Privacy Information Centre, by S. Lucey, Solicitor, G. Gilmore and A. Butler, Barristers-at-Law, and C. O’Dwyer, Senior Counsel,  
–        BSA Business Software Alliance Inc., by B. Van Vooren and K. Van Quathem, advocaten,  
–        Digitaleurope, by N. Cahill, Barrister, J. Cahir, Solicitor, and M. Cush, Senior Counsel,  
–        Ireland, by A. Joyce and M. Browne, acting as Agents, and D. Fennelly, Barrister-at-Law,  
–        the Belgian Government, by J.-C. Halleux and P. Cottin, acting as Agents,  
–        the Czech Government, by M. Smolek, J. Vláčil, O. Serdula and A. Kasalická, acting as Agents,  
–        the German Government, by J. Möller, D. Klebs and T. Henze, acting as Agents,  
–        the French Government, by A.-L. Desjonquères, acting as Agent,  
–        the Netherlands Government, by C.S. Schillemans, M.K. Bulterman and M. Noort, acting as Agents,  
–        the Austrian Government, by J. Schmoll and G. Kunnert, acting as Agents,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes, A. Pimenta and C. Vieira Guerra, acting as Agents,  
–        the United Kingdom Government, by S. Brandon, acting as Agent, and J. Holmes QC, and C. Knight, Barrister,  
–        the European Parliament, by M.J. Martínez Iglesias and A. Caiola, acting as Agents,  
–        the European Commission, by D. Nardi, H. Krämer and H. Kranenborg, acting as Agents,  
–        the European Data Protection Board (EDPB), by A. Jelinek and K. Behn, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 19 December 2019,  
gives the following  
Judgment  
1        This reference for a preliminary ruling, in essence, concerns:  
–        the interpretation of the first indent of Article 3(2), Articles 25 and 26 and Article 28(3) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), read in the light of Article 4(2) TEU and of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’);  
–        the interpretation and validity of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100) (‘the SCC Decision’); and  
–        the interpretation and validity of Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207, p. 1; ‘the Privacy Shield Decision’).  
2        The request has been made in proceedings between the Data Protection Commissioner (Ireland) (‘the Commissioner’), on the one hand, and Facebook Ireland Ltd and Maximillian Schrems, on the other, concerning a complaint brought by Mr Schrems concerning the transfer of his personal data by Facebook Ireland to Facebook Inc. in the United States.  
   
Legal context  
   
Directive 95/46  
3        Article 3 of Directive 95/46, under the heading ‘Scope’, stated, in paragraph 2:  
‘This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        …’  
4        Article 25 of that directive provided:  
‘1.      The Member States shall provide that the transfer to a third country of personal data … may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.  
2.      The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; …  
…  
6.      The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.  
Member States shall take the measures necessary to comply with the Commission’s Decision.’  
5        Article 26(2) and (4) of the directive provided:  
‘2.      Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.  
…  
4.      Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission’s decision.’  
6        Pursuant to Article 28(3) of that directive:  
‘Each authority shall in particular be endowed with:  
–        investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,  
–        effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,  
–        the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been infringed or to bring those infringements to the attention of the judicial authorities.  
…’  
   
The GDPR  
7        Directive 95/46 was repealed and replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
8        Recitals 6, 10, 101, 103, 104, 107 to 109, 114, 116 and 141 of the GDPR state:  
‘(6)      Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.  
…  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data (“sensitive data”). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.  
…  
(101)      Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in these flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.  
…  
(103)      The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.  
(104)      In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States’ data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.  
…  
(107)      The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.  
(108)      In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. …  
(109)      The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.  
…  
(114)      In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.  
…  
(116)      When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. …  
…  
(141)      Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. …’  
9        Article 2(1) and (2) of the GDPR provides:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;  
(c)      by a natural person in the course of a purely personal or household activity;  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
10      Article 4 of the GDPR provides:  
‘For the purposes of this Regulation:  
…  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;  
(8)      “processor”, means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;  
(9)      “recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;  
…’  
11      Article 23 of the GDPR states:  
‘1.      Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;  
…  
2.      In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:  
(a)      the purposes of the processing or categories of processing;  
(b)      the categories of personal data;  
(c)      the scope of the restrictions introduced;  
(d)      the safeguards to prevent abuse or unlawful access or transfer;  
(e)      the specification of the controller or categories of controllers;  
(f)      the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;  
(g)      the risks to the rights and freedoms of data subjects; and  
(h)      the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.’  
12      Chapter V of the GDPR, under the heading ‘Transfers of personal data to third countries or international organisations’, contains Articles 44 to 50 of that regulation. According to Article 44 thereof, under the heading ‘General principle for transfers’:  
‘Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.’  
13      Article 45 of the GDPR, under the heading ‘Transfers on the basis of an adequacy decision’, provides, in paragraphs 1 to 3:  
‘1.      A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.  
2.      When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:  
(a)      the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;  
(b)      the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and  
(c)      the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.  
3.      The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).’  
14      Article 46 of the GDPR, under the heading ‘Transfers subject to appropriate safeguards’, provides, in paragraphs 1 to 3:  
‘1.      In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.  
2.      The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:  
(a)      a legally binding and enforceable instrument between public authorities or bodies;  
(b)      binding corporate rules in accordance with Article 47;  
(c)      standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);  
(d)      standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);  
(e)      an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights; or  
(f)      an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.  
3.      Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:  
(a)      contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or  
(b)      provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.’  
15      Article 49 of the GDPR, under the heading ‘Derogations for specific situations’, states:  
‘1.      In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:  
(a)      the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;  
(b)      the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request;  
(c)      the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;  
(d)      the transfer is necessary for important reasons of public interest;  
(e)      the transfer is necessary for the establishment, exercise or defence of legal claims;  
(f)      the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;  
(g)      the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.  
Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.  
2.      A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.  
3.      Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.  
4.      The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.  
5.      In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.  
6.      The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.’  
16      Under Article 51(1) of the GDPR:  
‘Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (“supervisory authority”).’  
17      In accordance with Article 55(1) of the GDPR, ‘each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State’.  
18      Article 57(1) of that regulation states as follows:  
‘Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:  
(a)      monitor and enforce the application of this Regulation;  
…  
(f)      handle complaints lodged by a data subject … and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;  
…’  
19      According to Article 58(2) and (4) of the GDPR:  
‘2.      Each supervisory authority shall have all of the following corrective powers:  
…  
(f)      to impose a temporary or definitive limitation including a ban on processing;  
…  
(j)      to order the suspension of data flows to a recipient in a third country or to an international organisation.  
…  
4.      The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.’  
20      Article 64(2) of the GDPR states:  
‘Any supervisory authority, the Chair of the [European Data Protection Board (EDPB)] or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.’  
21      Under Article 65(1) of the GDPR:  
‘In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:  
…  
(c)      where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.’  
22      Article 77 of the GDPR, under the heading ‘Right to lodge a complaint with a supervisory authority’, states:  
‘1.      Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.  
2.      The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.’  
23      Article 78 of the GDPR, under the heading ‘Right to an effective judicial remedy against a supervisory authority’, provides, in paragraphs 1 and 2:  
‘1.      Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.  
2.      Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to [an] effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.’  
24      Article 94 of the GDPR provides:  
‘1.      Directive [95/46] is repealed with effect from 25 May 2018.  
2.      References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.’  
25      Pursuant to Article 99 of the GDPR:  
‘1.      This Regulation shall enter into force on the twentieth day following that of its publication in the   
Official Journal of the European Union  
.  
2.      It shall apply from 25 May 2018.’  
   
The   
SCC Decision  
26      Recital 11 of the SCC Decision reads as follows:  
‘Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject.’  
27      Article 1 of the SCC Decision states:  
‘The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive [95/46].’  
28      In accordance with the second paragraph of Article 2 of the SCC Decision, that decision ‘shall apply to the transfer of personal data by controllers established in the European Union to recipients established outside the territory of the European Union who act only as data processors’.  
29      Article 3 of the SCC Decision provides:  
‘For the purposes of this Decision, the following definitions shall apply:  
…  
(c)      “data exporter” means the controller who transfers the personal data;  
(d)      “data importer” means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter’s behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive [95/46];  
…  
(f)      “applicable data protection law” means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;  
…’  
30      According to its original wording, prior to the entry into force of Implementing Decision 2016/2297, Article 4 of Decision 2010/87 provided:  
‘1.      ‘Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive [95/46], the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:  
(a)      it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive [95/46] where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;  
(b)      a competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or  
(c)      there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.  
2.      The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.  
3.      When Member States adopt measures pursuant to paragraphs 1 and 2, they shall, without delay, inform the Commission which will forward the information to the other Member States.’  
31      Recital 5 of Implementing Decision 2016/2297, adopted after the judgment of 6 October 2015,   
Schrems  
 (C-362/14, EU:C:2015:650) was handed down, reads as follows:  
‘  
Mutatis mutandis  
, a Commission decision adopted pursuant to Article 26(4) of Directive [95/46] is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities, in so far as it has the effect of recognising that transfers taking place on the basis of standard contractual clauses set out therein offer sufficient safeguards as required by Article 26(2) of that Directive. This does not prevent a national supervisory authority from exercising its powers to oversee data flows, including the power to suspend or ban a transfer of personal data when it determines that the transfer is carried out in violation of EU or national data protection law, such as, for instance, when the data importer does not respect the standard contractual clauses.’  
32      According to its current wording, resulting from Implementing Decision 2016/2297, Article 4 of the SCC Decision states:  
‘Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive [95/46] leading to the suspension or definitive ban of data flows to third countries in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall, without delay, inform the Commission which will forward the information to the other Member States.’  
33      The annex to the SCC Decision, under the heading ‘Standard Contractual Clauses (Processors)’, is comprised of 12 standard clauses. Clause 3 thereof, itself under the heading ‘Third-party beneficiary clause’, provides:  
‘1.      The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.  
2.      The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.  
…’  
34      According to Clause 4 in that annex, under the heading ‘Obligations of the data exporter’:  
‘The data exporter agrees and warrants:  
(a)      that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;  
(b)      that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;  
…  
(f)      that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive [95/46];  
(g)      to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;  
…’  
35      Clause 5 in that annex, under the heading ‘Obligations of the data importer …’, provides:  
‘The data importer agrees and warrants:  
(a)      to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;  
(b)      that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;  
…  
(d)      that it will promptly notify the data exporter about:  
(i)      any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;  
(ii)      any accidental or unauthorised access; and  
(iii)      any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;  
…’  
36      The footnote to the heading of Clause 5 states:  
‘Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive [95/46], that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. …’  
37      Clause 6 in the annex to the SCC Decision, under the heading ‘Liability’, provides:  
‘1.      The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.  
2.      If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter …  
…’  
38      Clause 8 in that annex, under the heading ‘Cooperation with supervisory authorities’, stipulates, in paragraph 2 thereof:  
‘The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.’  
39      Clause 9 in that annex, under the heading ‘Governing law’, specifies that the clauses are to be governed by the law of the Member State in which the data exporter is established.  
40      According to Clause 11 in that annex, under the heading ‘Sub-processing’:  
‘1.      The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses …  
2.      The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.  
…’  
41      Clause 12 in the annex to the SCC Decision, under the heading ‘Obligation after the termination of personal data-processing services’, states, in paragraph 1 thereof:  
‘The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. …’  
   
The Privacy Shield Decision  
42      In the judgment of 6 October 2015,   
Schrems  
 (C-362/14, EU:C:2015:650), the Court declared Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7), in which the Commission had found that that third country ensured an adequate level of protection, invalid.  
43      Following the delivery of that judgment, the Commission adopted the Privacy Shield Decision, after having, for the purposes of adopting that decision, assessed the US legislation, as stated in recital 65 of the decision:  
‘The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. In addition, the U.S. government, through its Office of the Director of National Intelligence (ODNI) …, has provided the Commission with detailed representations and commitments that are contained in Annex VI to this decision. By letter signed by the Secretary of State and attached as Annex III to this decision the U.S. government has also committed to create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community. Finally, a representation from the U.S. Department of Justice, contained in Annex VII to this decision, describes the limitations and safeguards applicable to access and use of data by public authorities for law enforcement and other public interest purposes. In order to enhance transparency and to reflect the legal nature of these commitments, each of the documents listed and annexed to this decision will be published in the U.S. Federal Register.’  
44      The Commission’s assessment of those limitations and guarantees is summarised in recitals 67 to 135 of the Privacy Shield Decision, while the Commission’s conclusions on the adequate level of protection in the context of the EU-US Privacy Shield are set out in recitals 136 to 141 thereof.  
45      In particular, Recitals 68, 69, 76, 77, 109, 112 to 116, 120, 136 and 140 of the Privacy Shield Decision state:  
‘(68)      Under the U.S. Constitution, ensuring national security falls within the President’s authority as Commander in Chief, as Chief Executive and, as regards foreign intelligence, to conduct U.S. foreign affairs … While Congress has the power to impose limitations, and has done so in various respects, within these boundaries the President may direct the activities of the U.S. Intelligence Community, in particular through Executive Orders or Presidential Directives. … At present, the two central legal instruments in this regard are Executive Order 12333 (“E.O. 12333”) … and Presidential Policy Directive 28.  
(69)      Presidential Policy Directive 28 (“PPD-28”), issued on 17 January 2014, imposes a number of limitations for “signals intelligence” operations … This presidential directive has binding force for U.S. intelligence authorities … and remains effective upon change in the U.S. Administration … PPD-28 is of particular importance for non-US persons, including EU data subjects. …  
…  
(76)      Although not phrased in … legal terms, [the] principles [of PPD-28] capture the essence of the principles of necessity and proportionality. …  
(77)      As a directive issued by the President as the Chief Executive, these requirements bind the entire Intelligence Community and have been further implemented through agency rules and procedures that transpose the general principles into specific directions for day-to-day operations. …  
…  
(109)      Conversely, under Section 702 [of the Foreign Intelligence Surveillance Act (FISA)], the [United States Foreign Intelligence Surveillance Court (FISC)] does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the [US] Attorney General and the Director of National Intelligence [(DNI)]. … As indicated, the certifications to be approved by the FISC contain no information about the individual persons to be targeted but rather identify categories of foreign intelligence information … While the FISC does not assess — under a probable cause or any other standard — that individuals are properly targeted to acquire foreign intelligence information …, its control extends to the condition that “a significant purpose of the acquisition is to obtain foreign intelligence information” …  
…  
(112)      First, the [FISA] provides a number of remedies, available also to non-U.S. persons, to challenge unlawful electronic surveillance … This includes the possibility for individuals to bring a civil cause of action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed …; to sue U.S. government officials in their personal capacity (“under colour of law”) for money damages …; and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the United States …  
(113)      Second, the U.S. government referred the Commission to a number of additional avenues that EU data subjects could use to seek legal recourse against government officials for unlawful government access to, or use of, personal data, including for purported national security purposes …  
(114)      Finally, the U.S. government has pointed to the [Freedom of Information Act (FOIA)] as a means for non-U.S. persons to seek access to existing federal agency records, including where these contain the individual’s personal data … Given its focus, the FOIA does not provide an avenue for individual recourse against interference with personal data as such, even though it could in principle enable individuals to get access to relevant information held by national intelligence agencies. …  
(115)      While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available causes of action are limited … and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show “standing” …, which restricts access to ordinary courts …  
(116)      In order to provide for an additional redress avenue accessible for all EU data subjects, the U.S. government has decided to create a new Ombudsperson Mechanism as set out in the letter from the U.S. Secretary of State to the Commission which is contained in Annex III to this decision. This mechanism builds on the designation, under PPD-28, of a Senior Coordinator (at the level of Under-Secretary) in the State Department as a contact point for foreign governments to raise concerns regarding U.S. signals intelligence activities, but goes significantly beyond this original concept.  
…  
(120)      … the U.S. government commits to ensure that, in carrying out its functions, the Privacy Shield Ombudsperson will be able to rely on the cooperation from other oversight and compliance review mechanisms existing in U.S. law. … Where any non-compliance has been found by one of these oversight bodies, the Intelligence Community element (e.g. an intelligence agency) concerned will have to remedy the non-compliance as only this will allow the Ombudsperson to provide a “positive” response to the individual (i.e. that any non-compliance has been remedied) to which the U.S. government has committed. …  
…  
(136)      In the light of [those] findings, the Commission considers that the United States ensures an adequate level of protection for personal data transferred from the Union to self-certified organisations in the United States under the EU-U.S. Privacy Shield.  
…  
(140)      Finally, on the basis of the available information about the U.S. legal order, including the representations and commitments from the U.S. government, the Commission considers that any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference.’  
46      Under Article 1 of the Privacy Shield Decision:  
‘1.      For the purposes of Article 25(2) of [Directive 95/46], the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.  
2.      The EU-U.S. Privacy Shield is constituted by the Principles issued by the U.S. Department of Commerce on 7 July 2016 as set out in Annex II and the official representations and commitments contained in the documents listed in Annexes I [and] III to VII.  
3.      For the purpose of paragraph 1, personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the “Privacy Shield List”, maintained and made publicly available by the U.S. Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II.’  
47      Under the heading ‘EU-U.S. Privacy Shield Framework Principles issued by the U.S. Department of Commerce’, Annex II to the Privacy Shield Decision, provides, in paragraph I.5 thereof, that adherence to those principles may be limited, inter alia, ‘to the extent necessary to meet national security, public interest, or law enforcement requirements’.  
48      Annex III to that decision contains a letter from Mr John Kerry, then Secretary of State (United States), to the Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, to which a memorandum, Annex A, was attached, entitled ‘EU-U.S. Privacy Shield Ombudsperson mechanism regarding signals intelligence’, the latter of which contains the following passage:  
‘In recognition of the importance of the EU-U.S. Privacy Shield Framework, this Memorandum sets forth the process for implementing a new mechanism, consistent with [PPD-28], regarding signals intelligence …  
… President Obama announced the issuance of a new presidential directive — PPD-28 — to “clearly prescribe what we do, and do not do, when it comes to our overseas surveillance.”  
Section 4(d) of PPD-28 directs the Secretary of State to designate a “Senior Coordinator for International Information Technology Diplomacy” (Senior Coordinator) “to […] serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States.” …  
…  
1.      … The Senior Coordinator will serve as the Privacy Shield Ombudsperson and … will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Ombudsperson is independent from the Intelligence Community. The Ombudsperson reports directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided.  
…’  
49      Annex VI to the Privacy Shield Decision contains a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, in which it is stated that PPD-28 allows for ‘“bulk” collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection’.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
50      Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network (‘Facebook’) since 2008.  
51      Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his or her registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland’s users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.  
52      On 25 June 2013, Mr Schrems filed a complaint with the Commissioner whereby he requested, in essence, that Facebook Ireland be prohibited from transferring his personal data to the United States, on the ground that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities in which the public authorities were engaged. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520, the Commission had found that the United States ensured an adequate level of protection.  
53      The High Court (Ireland), before which Mr Schrems had brought judicial review proceedings against the rejection of his complaint, made a request to the Court for a preliminary ruling on the interpretation and validity of Decision 2000/520. In a judgment of 6 October 2015,   
Schrems  
 (C-362/14, EU:C:2015:650), the Court declared that decision invalid.  
54      Following that judgment, the referring court annulled the rejection of Mr Schrems’s complaint and referred that decision back to the Commissioner. In the course of the Commissioner’s investigation, Facebook Ireland explained that a large part of personal data was transferred to Facebook Inc. pursuant to the standard data protection clauses set out in the annex to the SCC Decision. On that basis, the Commissioner asked Mr Schrems to reformulate his complaint.  
55      In his reformulated complaint lodged on 1 December 2015, Mr Schrems claimed, inter alia, that United States law requires Facebook Inc. to make the personal data transferred to it available to certain United States authorities, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). He submitted that, since that data was used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter, the SCC Decision cannot justify the transfer of that data to the United States. In those circumstances, Mr Schrems asked the Commissioner to prohibit or suspend the transfer of his personal data to Facebook Inc.  
56      On 24 May 2016, the Commissioner published a ‘draft decision’ summarising the provisional findings of her investigation. In that draft decision, she took the provisional view that the personal data of EU citizens transferred to the United States were likely to be consulted and processed by the US authorities in a manner incompatible with Articles 7 and 8 of the Charter and that US law did not provide those citizens with legal remedies compatible with Article 47 of the Charter. The Commissioner found that the standard data protection clauses in the annex to the SCC Decision are not capable of remedying that defect, since they confer only contractual rights on data subjects against the data exporter and importer, without, however, binding the United States authorities.  
57      Taking the view that, in those circumstances, Mr Schrems’s reformulated complaint raised the issue of the validity of the SCC Decision, on 31 May 2016, the Commissioner brought an action before the High Court, relying on the case-law arising from the judgment of 6 October 2015,   
Schrems  
 (C-362/14, EU:C:2015:650, paragraph 65), in order for the High Court to refer a question on that issue to the Court. By order of 4 May 2018, the High Court made the present reference for a preliminary ruling to the Court.  
58      In an annex to the order for reference, the High Court provided a copy of a judgment handed down on 3 October 2017, in which it had set out the results of an examination of the evidence produced before it in the national proceedings, in which the US Government had participated.  
59      In that judgment, to which the request for a preliminary ruling refers on several occasions, the referring court stated that, as a matter of principle, it is not only entitled, but is obliged, to consider all of the facts and arguments presented to it and to decide on the basis of those facts and arguments whether or not a reference is required. The High Court considers that, in any event, it is required to take into account any amendments that may have occurred in the interval between the institution of the proceedings and the hearing which it held. That court stated that, in the main proceedings, its own assessment is not confined to the grounds of invalidity put forward by the Commissioner, as a result of which it may of its own motion decide that there are other well-founded grounds of invalidity and, on those grounds, refer questions for a preliminary ruling.  
60      According to the findings in that judgment, the US authorities’ intelligence activities concerning the personal data transferred to the United States are based, inter alia, on Section 702 of the FISA and on E.O. 12333.  
61      In its judgment, the referring court specifies that Section 702 of the FISA permits the Attorney General and the Director of National Intelligence to authorise jointly, following FISC approval, the surveillance of individuals who are not United States citizens located outside the United States in order to obtain ‘foreign intelligence information’, and provides, inter alia, the basis for the PRISM and UPSTREAM surveillance programmes. In the context of the PRISM programme, Internet service providers are required, according to the findings of that court, to supply the NSA with all communications to and from a ‘selector’, some of which are also transmitted to the FBI and the Central Intelligence Agency (CIA).  
62      As regards the UPSTREAM programme, that court found that, in the context of that programme, telecommunications undertakings operating the ‘backbone’ of the Internet — that is to say, the network of cables, switches and routers — are required to allow the NSA to copy and filter Internet traffic flows in order to acquire communications from, to or about a non-US national associated with a ‘selector’. Under that programme, the NSA has, according to the findings of that court, access both to the metadata and to the content of the communications concerned.  
63      The referring court found that E.O. 12333 allows the NSA to access data ‘in transit’ to the United States, by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States and being subject there to the FISA. It adds that activities conducted pursuant to E.O. 12333 are not governed by statute.  
64      As regards the limits on intelligence activities, the referring court emphasises the fact that non-US persons are covered only by PPD-28, which merely states that intelligence activities should be ‘as tailored as feasible’. On the basis of those findings, the referring court considers that the United States carries out mass processing of personal data without ensuring a level of protection essentially equivalent to that guaranteed by Articles 7 and 8 of the Charter.  
65      As regards judicial protection, the referring court states that EU citizens do not have the same remedies as US citizens in respect of the processing of personal data by the US authorities, since the Fourth Amendment to the Constitution of the United States, which constitutes, in United States law, the most important cause of action available to challenge unlawful surveillance, does not apply to EU citizens. In that regard, the referring court states that there are substantial obstacles in respect of the causes of action open to EU citizens, in particular that of   
locus standi  
, which it considers to be excessively difficult to satisfy. Furthermore, according to the findings of the referring court, the NSA’s activities based on E.O. 12333 are not subject to judicial oversight and are not justiciable. Lastly, the referring court considers that, in so far as, in its view, the Privacy Shield Ombudsperson is not a tribunal within the meaning of Article 47 of the Charter, US law does not afford EU citizens a level of protection essentially equivalent to that guaranteed by the fundamental right enshrined in that article.  
66      In its request for reference preliminary ruling, the referring court also states that the parties to the main proceedings disagree, inter alia, on the applicability of EU law to transfers to a third country of personal data which are likely to be processed by the authorities of that country, inter alia, for purposes of national security and on the factors to be taken into consideration for the purposes of assessing whether that country ensures an adequate level of protection. In particular, that court notes that, according to Facebook Ireland, the Commission’s findings on the adequacy of the level of protection ensured by a third country, such as those set out in the Privacy Shield Decision, are also binding on the supervisory authorities in the context of a transfer of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision.  
67      As regards those standard data protection clauses, that court asks whether the SCC Decision may be considered to be valid, despite the fact that, according to that court, those clauses are not binding on the State authorities of the third country concerned and, therefore, are not capable of remedying a possible lack of an adequate level of protection in that country. In that regard, it considers that the possibility, afforded to the competent authorities in the Member States by Article 4(1)(a) of Decision 2010/87, in its version prior to the entry into force of Implementing Decision 2016/2297, of prohibiting transfers of personal data to a third country that imposes requirements on the importer that are incompatible with the guarantees contained in those clauses, demonstrates that the state of the law in the third country can justify prohibiting the transfer of data, even when carried out pursuant to the standard data protection clauses in the annex to the SCC Decision, and therefore makes clear that those requirements may be insufficient in ensuring an adequate level of protection. Nonetheless, the referring court harbours doubts as to the extent of the Commissioner’s power to prohibit a transfer of data based on those clauses, despite taking the view that discretion cannot be sufficient to ensure adequate protection.  
68      In those circumstances, the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
(1)      In circumstances in which personal data is transferred by a private company from a European Union (EU) Member State to a private company in a third country for a commercial purpose pursuant to [the SCC Decision] and may be further processed in the third country by its authorities for purposes of national security but also for purposes of law enforcement and the conduct of the foreign affairs of the third country, does EU law (including the Charter) apply to the transfer of the data notwithstanding the provisions of Article 4(2) TEU in relation to national security and the provisions of the first indent of Article 3(2) of Directive [95/46] in relation to public security, defence and State security?  
(2)      (a)      In determining whether there is a violation of the rights of an individual through the transfer of data from the [European Union] to a third country under the [SCC Decision] where it may be further processed for national security purposes, is the relevant comparator for the purposes of [Directive 95/46]:  
(i)      the Charter, the EU Treaty, the FEU Treaty, [Directive 95/46], the [European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950] (or any other provision of EU law); or  
(ii)      the national laws of one or more Member States?  
(b)      If the relevant comparator is (ii), are the practices in the context of national security in one or more Member States also to be included in the comparator?  
(3)      When assessing whether a third country ensures the level of protection required by EU law to personal data transferred to that country for the purposes of Article 26 of [Directive 95/46], ought the level of protection in the third country be assessed by reference to:  
(a)      the applicable rules in the third country resulting from its domestic law or international commitments, and the practice designed to ensure compliance with those rules, to include the professional rules and security measures which are complied with in the third country;  
or  
(b)      the rules referred to in (a) together with such administrative, regulatory and compliance practices and policy safeguards, procedures, protocols, oversight mechanisms and non-judicial remedies as are in place in the third country?  
(4)      Given the facts found by the High Court in relation to US law, if personal data is transferred from the European Union to the United States under [the SCC Decision] does this violate the rights of individuals under Articles 7 and/or 8 of the Charter?  
(5)      Given the facts found by the High Court in relation to US law, if personal data is transferred from the European Union to the United States under [the SCC Decision]:  
(a)      does the level of protection afforded by the United States respect the essence of an individual’s right to a judicial remedy for breach of his or her data privacy rights guaranteed by Article 47 of the Charter?  
If the answer to Question 5(a) is in the affirmative:  
(b)      are the limitations imposed by US law on an individual’s right to a judicial remedy in the context of US national security proportionate within the meaning of Article 52 of the Charter and do not exceed what is necessary in a democratic society for national security purposes?  
(6)      (a)      What is the level of protection required to be afforded to personal data transferred to a third country pursuant to standard contractual clauses adopted in accordance with a decision of the Commission under Article 26(4) [of Directive 95/46] in light of the provisions of [Directive 95/46] and in particular Articles 25 and 26 read in the light of the Charter?  
(b)      What are the matters to be taken into account in assessing whether the level of protection afforded to data transferred to a third country under [the SCC Decision] satisfies the requirements of [Directive 95/46] and the Charter?  
(7)      Does the fact that the standard contractual clauses apply as between the data exporter and the data importer and do not bind the national authorities of a third country who may require the data importer to make available to its security services for further processing the personal data transferred pursuant to the clauses provided for in [the SCC Decision] preclude the clauses from adducing adequate safeguards as envisaged by Article 26(2) of [Directive 95/46]?  
(8)      If a third country data importer is subject to surveillance laws that in the view of a data protection authority conflict with the [standard contractual clauses] or Article 25 and 26 of [Directive 95/46] and/or the Charter, is a data protection authority required to use its enforcement powers under Article 28(3) of [Directive 95/46] to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of recital 11 of [the SCC Decision], or can a data protection authority use its discretion not to suspend data flows?  
(9)      (a)      For the purposes of Article 25(6) of [Directive 95/46], does [the Privacy Shield Decision] constitute a finding of general application binding on data protection authorities and the courts of the Member States to the effect that the United States ensures an adequate level of protection within the meaning of Article 25(2) of [Directive 95/46] by reason of its domestic law or of the international commitments it has entered into?  
(b)      If it does not, what relevance, if any, does the Privacy Shield Decision have in the assessment conducted into the adequacy of the safeguards provided to data transferred to the United States which is transferred pursuant to the [SCC Decision]?  
(10)      Given the findings of the High Court in relation to US law, does the provision of the Privacy Shield ombudsperson under Annex A to Annex III to the Privacy Shield Decision when taken in conjunction with the existing regime in the United States ensure that the US provides a remedy to data subjects whose personal data is transferred to the United States under the [SCC Decision] that is compatible with Article 47 of the Charter]?  
(11)      Does the [SCC Decision] violate Articles 7, 8 and/or 47 of the Charter?’  
   
Admissibility of the request for a preliminary ruling  
69      Facebook Ireland and the German and United Kingdom Governments claim that the request for a preliminary ruling is inadmissible.  
70      With regard to the objection raised by Facebook Ireland, that company observes that the provisions of Directive 95/46, on which the questions referred for a preliminary ruling are based, were repealed by the GDPR.  
71      In that regard, although Directive 95/46 was, under Article 94(1) of the GDPR, repealed with effect from 25 May 2018, that directive was still in force when, on 4 May 2018, the present request for a preliminary ruling, received at the Court on 9 May 2018, was made. In addition, the first indent of Article 3(2) and Articles 25, 26 and 28(3) of Directive 95/46 cited in the questions referred, were, in essence, reproduced in Article 2(2) and Articles 45, 46 and 58 of the GDPR, respectively. Furthermore, it must be borne in mind that the Court has a duty to interpret all provisions of EU law which national courts require in order to decide the actions pending before them, even if those provisions are not expressly indicated in the questions referred to the Court of Justice by those courts (judgment of 2 April 2020,   
Ruska Federacija  
, C-897/19 PPU, EU:C:2020:262, paragraph 43 and the case-law cited). On those grounds, the fact that the referring court referred its questions by reference solely to the provisions of Directive 95/46 cannot render the present request for a preliminary ruling inadmissible.  
72      For its part, the German Government bases its objection of inadmissibility on the fact, first, that the Commissioner merely expressed doubts, and not a definitive opinion, as to the validity of the SCC Decision and, second, that the referring court failed to ascertain whether Mr Schrems had unambiguously given his consent to the transfers of data at issue in the main proceedings, which, if that had been the case, would have the effect of rendering an answer to that question redundant. Lastly, the United Kingdom Government maintains that the questions referred for a preliminary ruling are hypothetical since that court did not find that that data had actually been transferred on the basis of that decision.  
73      It follows from settled case-law of the Court that it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions referred concern the interpretation or the validity of a rule of EU law, the Court is in principle bound to give a ruling. It follows that questions referred by national courts enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court only where it appears that the interpretation sought bears no relation to the actual facts of the main action or its object, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgments of 16 June 2015,   
Gauweiler and Others  
, C-62/14, EU:C:2015:400, paragraphs 24 and 25; of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 45; and of 19 December 2019,   
Dobersberger  
, C-16/18, EU:C:2019:1110, paragraphs 18 and 19).  
74      In the present case, the request for a preliminary ruling contains sufficient factual and legal material to understand the significance of the questions referred. Furthermore, and most importantly, nothing in the file before the Court leads to the conclusion that the interpretation of EU law that is requested is unrelated to the actual facts of the main action or its object, or that the problem is hypothetical, inter alia, on the basis that the transfer of the personal data at issue in the main proceedings may have been based on the express consent of the data subject of that transfer rather than based on the SCC Decision. As indicated in the request for a preliminary ruling, Facebook Ireland has acknowledged that it transfers the personal data of its subscribers residing in the European Union to Facebook Inc. and that those transfers, the lawfulness of which Mr Schrems disputes, were in large part carried out pursuant to the standard data protection clauses in the annex to the SCC Decision.  
75      Moreover, it is irrelevant to the admissibility of the present request for a preliminary ruling that the Commissioner did not express a definitive opinion on the validity of that decision in so far as the referring court considers that an answer to the questions referred for a preliminary ruling concerning the interpretation and validity of rules of EU law is necessary in order to dispose of the case in the main proceedings.  
76      It follows that the request for a preliminary ruling is admissible.  
   
Consideration of the questions referred  
77      As a preliminary matter, it must be borne in mind that the present request for a preliminary ruling has arisen following a complaint made by Mr Schrems requesting that the Commissioner order the suspension or prohibition, in the future, of the transfer by Facebook Ireland of his personal data to Facebook Inc. Although the questions referred for a preliminary ruling refer to the provisions of Directive 95/46, it is common ground that the Commissioner had not yet adopted a final decision on that complaint when that directive was repealed and replaced by the GDPR with effect from 25 May 2018.  
78      That absence of a national decision distinguishes the situation at issue in the main proceedings from those which gave rise to the judgments of 24 September 2019,   
Google (Territorial scope of de-referencing)  
 (C-507/17, EU:C:2019:772), and of 1 October 2019,   
Planet49  
 (C-673/17, EU:C:2019:801), in which decisions adopted prior to the repeal of that directive were at issue.  
79      The questions referred for a preliminary ruling must therefore be answered in the light of the provisions of the GDPR rather than those of Directive 95/46.  
   
The first question  
80      By its first question, the referring court wishes to know, in essence, whether Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR, read in conjunction with Article 4(2) TEU, must be interpreted as meaning that that regulation applies to the transfer of personal data by an economic operator established in a Member State to another economic operator established in a third country, in circumstances where, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of that third country for the purposes of public security, defence and State security.  
81      In that regard, it should be made clear at the outset that the rule in Article 4(2) TEU, according to which, within the European Union, national security remains the sole responsibility of each Member State, concerns Member States of the European Union only. That rule is therefore irrelevant, in the present case, for the purposes of interpreting Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR.  
82      Under Article 2(1) of the GDPR, that regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Article 4(2) of that regulation defines ‘processing’ as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means’ and mentions, by way of example, ‘disclosure by transmission, dissemination or otherwise making available’, but does not distinguish between operations which take place within the European Union and those which are connected with a third country. Furthermore, the GDPR subjects transfers of personal data to third countries to specific rules in Chapter V thereof, entitled ‘Transfers of personal data to third countries or international organisations’, and also confers specific powers on the supervisory authorities for that purpose, which are set out in Article 58(2)(j) of that regulation.  
83      It follows that the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 4(2) of the GDPR, carried out in a Member State, and falls within the scope of that regulation under Article 2(1) thereof (see, by analogy, as regards Article 2(b) and Article 3(1) of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 45 and the case-law cited).  
84      As to whether such an operation may be regarded as being excluded from the scope of the GDPR under Article 2(2) thereof, it should be noted that that provision lays down exceptions to the scope of that regulation, as defined in Article 2(1) thereof, which must be interpreted strictly (see, by analogy, as regards Article 3(2) of Directive 95/46, judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 37 and the case-law cited).  
85      In the present case, since the transfer of personal data at issue in the main proceedings is from Facebook Ireland to Facebook Inc., namely between two legal persons, that transfer does not fall within Article 2(2)(c) of the GDPR, which refers to the processing of data by a natural person in the course of a purely personal or household activity. Such a transfer also does not fall within the exceptions laid down in Article 2(2)(a), (b) and (d) of that regulation, since the activities mentioned therein by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (see, by analogy, as regards Article 3(2) of Directive 95/46, judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 38 and the case-law cited).  
86      The possibility that the personal data transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing for the purposes of public security, defence and State security by the authorities of that third country cannot remove that transfer from the scope of the GDPR.  
87      Indeed, by expressly requiring the Commission, when assessing the adequacy of the level of protection afforded by a third country, to take account, inter alia, of ‘relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation’, it is patent from the very wording of Article 45(2)(a) of that regulation that no processing by a third country of personal data for the purposes of public security, defence and State security excludes the transfer at issue from the application of the regulation.  
88      It follows that such a transfer cannot fall outside the scope of the GDPR on the ground that the data at issue is liable to be processed, at the time of that transfer or thereafter, by the authorities of the third country concerned, for the purposes of public security, defence and State security.  
89      Therefore, the answer to the first question is that Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.  
   
The second, third and sixth questions  
90      By its second, third and sixth questions, the referring court seeks clarification from the Court, in essence, on the level of protection required by Article 46(1) and Article 46(2)(c) of the GDPR in respect of a transfer of personal data to a third country based on standard data protection clauses. In particular, the referring court asks the Court to specify which factors need to be taken into consideration for the purpose of determining whether that level of protection is ensured in the context of such a transfer.  
91      As regards the level of protection required, it follows from a combined reading of those provisions that, in the absence of an adequacy decision under Article 45(3) of that regulation, a controller or processor may transfer personal data to a third country only if the controller or processor has provided ‘appropriate safeguards’, and on condition that ‘enforceable data subject rights and effective legal remedies for data subjects’ are available, such safeguards being able to be provided, inter alia, by the standard data protection clauses adopted by the Commission.  
92      Although Article 46 of the GDPR does not specify the nature of the requirements which flow from that reference to ‘appropriate safeguards’, ‘enforceable rights’ and ‘effective legal remedies’, it should be noted that that article appears in Chapter V of that regulation and, accordingly, must be read in the light of Article 44 of that regulation, entitled ‘General principle for transfers’, which lays down that ‘all provisions [in that chapter] shall be applied in order to ensure that the level of protection of natural persons guaranteed by [that regulation] is not undermined’. That level of protection must therefore be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.  
93      As the Advocate General stated in point 117 of his Opinion, the provisions of Chapter V of the GDPR are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country, in accordance with the objective set out in recital 6 thereof.  
94      The first sentence of Article 45(1) of the GDPR provides that a transfer of personal data to a third country may be authorised by a Commission decision to the effect that that third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection. In that regard, although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term ‘adequate level of protection’ must, as confirmed by recital 104 of that regulation, be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph would be undermined (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 73).  
95      In that context, recital 107 of the GDPR states that, where ‘a third country, a territory or a specified sector within a third country … no longer ensures an adequate level of data protection. … the transfer of personal data to that third country … should be prohibited, unless the requirements [of that regulation] relating to transfers subject to appropriate safeguards … are fulfilled’. To that effect, recital 108 of the regulation states that, in the absence of an adequacy decision, the appropriate safeguards to be taken by the controller or processor in accordance with Article 46(1) of the regulation must ‘compensate for the lack of data protection in a third country’ in order to ‘ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union’.  
96      It follows, as the Advocate General stated in point 115 of his Opinion, that such appropriate guarantees must be capable of ensuring that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially equivalent to that which is guaranteed within the European Union.  
97      The referring court also asks whether the level of protection essentially equivalent to that guaranteed within the European Union must be determined in the light of EU law, in particular the rights guaranteed by the Charter and/or the fundamental rights enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms (‘the ECHR’), or in the light of the national law of the Member States.  
98      In that regard, it should be noted that, although, as Article 6(3) TEU confirms, the fundamental rights enshrined in the ECHR constitute general principles of EU law and although Article 52(3) of the Charter provides that the rights contained in the Charter which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that convention, the latter does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law (judgments of 26 February 2013,   
Åkerberg Fransson  
, C-617/10, EU:C:2013:105, paragraph 44 and the case-law cited, and of 20 March 2018,   
Menci  
, C-524/15, EU:C:2018:197, paragraph 22).  
99      In those circumstances, the Court has held that the interpretation of EU law and examination of the legality of EU legislation must be undertaken in the light of the fundamental rights guaranteed by the Charter (see, by analogy, judgment of 20 March 2018,   
Menci  
, C-524/15, EU:C:2018:197, paragraph 24).  
100    Furthermore, the Court has consistently held that the validity of provisions of EU law and, in the absence of an express reference to the national law of the Member States, their interpretation, cannot be construed in the light of national law, even national law of constitutional status, in particular fundamental rights as formulated in the national constitutions (see, to that effect, judgments of 17 December 1970,   
Internationale Handelsgesellschaft  
, 11/70, EU:C:1970:114, paragraph 3; of 13 December 1979,   
Hauer  
, 44/79, EU:C:1979:290, paragraph 14; and of 18 October 2016,   
Nikiforidis  
, C-135/15, EU:C:2016:774, paragraph 28 and the case-law cited).  
101    It follows that, since, first, a transfer of personal data, such as that at issue in the main proceedings, for commercial purposes by an economic operator established in one Member State to another economic operator established in a third country, falls, as is apparent from the answer to the first question, within the scope of the GDPR and, second, the purpose of that regulation is, inter alia, as is apparent from recital 10 thereof, to ensure a consistent and high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union, the level of protection of fundamental rights required by Article 46(1) of that regulation must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter.  
102    The referring court also seeks to ascertain what factors should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to standard data protection clauses adopted under Article 46(2)(c) of the GDPR.  
103    In that regard, although that provision does not list the various factors which must be taken into consideration for the purposes of assessing the adequacy of the level of protection to be observed in such a transfer, Article 46(1) of that regulation states that data subjects must be afforded appropriate safeguards, enforceable rights and effective legal remedies.  
104    The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.  
105    Therefore, the answer to the second, third and sixth questions is that Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.  
   
The eighth question  
106    By its eighth question, the referring court wishes to know, in essence, whether Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that the competent supervisory authority is required to suspend or prohibit a transfer of personal data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured, or as meaning that the exercise of those powers is limited to exceptional cases.  
107    In accordance with Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data. Each of those authorities is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down in that regulation (see, by analogy, as regards Article 28 of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 47).  
108    It follows from those provisions that the supervisory authorities’ primary responsibility is to monitor the application of the GDPR and to ensure its enforcement. The exercise of that responsibility is of particular importance where personal data is transferred to a third country since, as is clear from recital 116 of that regulation, ‘when personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information’. In such cases, as is stated in that recital, ‘supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders’.  
109    In addition, under Article 57(1)(f) of the GDPR, each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that data subject considers that the processing of his or her personal data infringes the regulation, and is required to examine the nature of that complaint as necessary. The supervisory authority must handle such a complaint with all due diligence (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 63).  
110    Article 78(1) and (2) of the GDPR recognises the right of each person to an effective judicial remedy, in particular, where the supervisory authority fails to deal with his or her complaint. Recital 141 of that regulation also refers to that ‘right to an effective judicial remedy in accordance with Article 47 of the Charter’ in circumstances where that supervisory authority ‘does not act where such action is necessary to protect the rights of the data subject’.  
111    In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt.  
112    Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence.  
113    In that regard, as the Advocate General also stated in point 148 of his Opinion, the supervisory authority is required, under Article 58(2)(f) and (j) of that regulation, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.  
114    The interpretation in the previous paragraph is not undermined by the Commissioner’s reasoning that Article 4 of Decision 2010/87, in its version prior to the entry into force of Implementing Decision 2016/2297, read in the light of recital 11 of that decision, confined the power of supervisory authorities to suspend or prohibit a transfer of personal data to a third country to certain exceptional circumstances. As amended by Implementing Decision 2016/2297, Article 4 of the SCC Decision refers to the power of the supervisory authorities, now under Article 58(2)(f) and (j) of the GDPR, to suspend or ban such a transfer, without confining the exercise of that power to exceptional circumstances.  
115    In any event, the implementing power which Article 46(2)(c) of the GDPR grants to the Commission for the purposes of adopting standard data protection clauses does not confer upon it competence to restrict the national supervisory authorities’ powers on the basis of Article 58(2) of that regulation (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraphs 102 and 103). Moreover, as stated in recital 5 of Implementing Decision 2016/2297, the SCC Decision ‘does not prevent a [supervisory authority] from exercising its powers to oversee data flows, including the power to suspend or ban a transfer of personal data when it determines that the transfer is carried out in violation of EU or national data protection law’.  
116    It should, however, be pointed out that the powers of the competent supervisory authority are subject to full compliance with the decision in which the Commission finds, where relevant, under the first sentence of Article 45(1) of the GDPR, that a particular third country ensures an adequate level of protection. In such a case, it is clear from the second sentence of Article 45(1) of that regulation, read in conjunction with recital 103 thereof, that transfers of personal data to the third country in question may take place without requiring any specific authorisation.  
117    Under the fourth paragraph of Article 288 TFEU, a Commission adequacy decision is, in its entirety, binding on all the Member States to which it is addressed and is therefore binding on all their organs in so far as it finds that the third country in question ensures an adequate level of protection and has the effect of authorising such transfers of personal data (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 51 and the case-law cited).  
118    Thus, until such time as a Commission adequacy decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection (judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 52 and the case-law cited) and, as a result, to suspend or prohibit transfers of personal data to that third country.  
119    However, a Commission adequacy decision adopted pursuant to Article 45(3) of the GDPR cannot prevent persons whose personal data has been or could be transferred to a third country from lodging a complaint, within the meaning of Article 77(1) of the GDPR, with the competent national supervisory authority concerning the protection of their rights and freedoms in regard to the processing of that data. Similarly, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 53).  
120    Thus, even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of his or her rights and freedoms in regard to the processing of personal data relating to him or her, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraphs 57 and 65).  
121    In the light of the foregoing considerations, the answer to the eighth question is that Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that, unless there is a valid Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.  
   
The  
7th and 11th  
 questions  
122    By its 7th and 11th questions, which it is appropriate to consider together, the referring court seeks clarification from the Court, in essence, on the validity of the SCC Decision in the light of Articles 7, 8 and 47 of the Charter.  
123    In particular, as is clear from the wording of the seventh question and the corresponding explanations in the request for a preliminary ruling, the referring court asks whether the SCC Decision is capable of ensuring an adequate level of protection of the personal data transferred to third countries given that the standard data protection clauses provided for in that decision do not bind the supervisory authorities of those third countries.  
124    Article 1 of the SCC Decision provides that the standard data protection clauses set out in its annex are considered to offer adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals in accordance with the requirements of Article 26(2) of Directive 95/46. The latter provision was, in essence, reproduced in Article 46(1) and Article 46(2)(c) of the GDPR.  
125    However, although those clauses are binding on a controller established in the European Union and the recipient of the transfer of personal data established in a third country where they have concluded a contract incorporating those clauses, it is common ground that those clauses are not capable of binding the authorities of that third country, since they are not party to the contract.  
126    Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.  
127    Thus, the question arises whether a Commission decision concerning standard data protection clauses, adopted pursuant to Article 46(2)(c) of the GDPR, is invalid in the absence, in that decision, of guarantees which can be enforced against the public authorities of the third countries to which personal data is or could be transferred pursuant to those clauses.  
128    Article 46(1) of the GDPR provides that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. According to Article 46(2)(c) of the GDPR, those safeguards may be provided by standard data protection clauses drawn up by the Commission. However, those provisions do not state that all safeguards must necessarily be provided for in a Commission decision such as the SCC Decision.  
129    It should be noted in that regard that such a standard clauses decision differs from an adequacy decision adopted pursuant to Article 45(3) of the GDPR, which seeks, following an examination of the legislation of the third country concerned taking into account, inter alia, the relevant legislation on national security and public authorities’ access to personal data, to find with binding effect that a third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection and that the access of that third country’s public authorities to such data does not therefore impede transfers of such personal data to the third country. Such an adequacy decision can therefore be adopted by the Commission only if it has found that the third country’s relevant legislation in that field does in fact provide all the necessary guarantees from which it can be concluded that that legislation ensures an adequate level of protection.  
130    By contrast, in the case of a Commission decision adopting standard data protection clauses, such as the SCC Decision, in so far as such a decision does not refer to a third country, a territory or one or more specific sectors in a third country, it cannot be inferred from Article 46(1) and Article 46(2)(c) of the GDPR that the Commission is required, before adopting such a decision, to assess the adequacy of the level of protection ensured by the third countries to which personal data could be transferred pursuant to such clauses.  
131    In that regard, it must be borne in mind that, according to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, it is for the controller or processor established in the European Union to provide, inter alia, appropriate safeguards. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor ‘should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject’ and that ‘those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies … in the Union or in a third country’.  
132    Since by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries, as is clear from paragraph 125 above, but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by that regulation is not undermined, it may prove necessary to supplement the guarantees contained in those standard data protection clauses. In that regard, recital 109 of the regulation states that ‘the possibility for the controller … to use standard data-protection clauses adopted by the Commission … should [not] prevent [it] … from adding other clauses or additional safeguards’ and states, in particular, that the controller ‘should be encouraged to provide additional safeguards … that supplement standard [data] protection clauses’.  
133    It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.  
134    In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.  
135    Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.  
136    Therefore, the mere fact that standard data protection clauses in a Commission decision adopted pursuant to Article 46(2)(c) of the GDPR, such as those in the annex to the SCC Decision, do not bind the authorities of third countries to which personal data may be transferred cannot affect the validity of that decision.  
137    That validity depends, however, on whether, in accordance with the requirement of Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, such a standard clauses decision incorporates effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to the clauses of such a decision are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.  
138    As regards the guarantees contained in the standard data protection clauses in the annex to the SCC Decision, it is clear from Clause 4(a) and (b), Clause 5(a), Clause 9 and Clause 11(1) thereof that a data controller established in the European Union, the recipient of the personal data and any processor thereof mutually undertake to ensure that the processing of that data, including the transfer thereof, has been and will continue to be carried out in accordance with ‘the applicable data protection law’, namely, according to the definition set out in Article 3(f) of that decision, ‘the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established’. The provisions of the GDPR, read in the light of the Charter, form part of that legislation.  
139    In addition, a recipient of personal data established in a third country undertakes, pursuant to Clause 5(a), to inform the controller established in the European Union promptly of any inability to comply with its obligations under the contract concluded. In particular, according to Clause 5(b), the recipient certifies that it has no reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under the contract entered into and undertakes to notify the data controller about any change in the national legislation applicable to it which is likely to have a substantial adverse effect on the warranties and obligations provided by the standard data protection clauses in the annex to the SCC Decision, promptly upon notice thereof. Furthermore, although Clause 5(d)(i) allows a recipient of personal data not to notify a controller established in the European Union of a legally binding request for disclosure of the personal data by a law enforcement authority, in the event of legislation prohibiting that recipient from doing so, such as a prohibition under criminal law the aim of which is to preserve the confidentiality of a law enforcement investigation, the recipient is nevertheless required, pursuant to Clause 5(a) in the annex to the SCC Decision, to inform the controller of his or her inability to comply with the standard data protection clauses.  
140    Clause 5(a) and (b), in both cases to which it refers, confers on the controller established in the European Union the right to suspend the transfer of data and/or to terminate the contract. In the light of the requirements of Article 46(1) and (2)(c) of the GDPR, read in the light of Articles 7 and 8 of the Charter, the controller is bound to suspend the transfer of data and/or to terminate the contract where the recipient is not, or is no longer, able to comply with the standard data protection clauses. Unless the controller does so, it will be in breach of its obligations under Clause 4(a) in the annex to the SCC Decision as interpreted in the light of the GDPR and of the Charter.  
141    It follows that Clause 4(a) and Clause 5(a) and (b) in that annex oblige the controller established in the European Union and the recipient of personal data to satisfy themselves that the legislation of the third country of destination enables the recipient to comply with the standard data protection clauses in the annex to the SCC Decision, before transferring personal data to that third country. As regards that verification, the footnote to Clause 5 states that mandatory requirements of that legislation which do not go beyond what is necessary in a democratic society to safeguard, inter alia, national security, defence and public security are not in contradiction with those standard data protection clauses. Conversely, as stated by the Advocate General in point 131 of his Opinion, compliance with an obligation prescribed by the law of the third country of destination which goes beyond what is necessary for those purposes must be treated as a breach of those clauses. Operators’ assessments of the necessity of such an obligation must, where relevant, take into account a finding that the level of protection ensured by the third country in a Commission adequacy decision, adopted under Article 45(3) of the GDPR, is appropriate.  
142    It follows that a controller established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. The recipient is, where appropriate, under an obligation, under Clause 5(b), to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract.  
143    If the recipient of personal data to a third country has notified the controller, pursuant to Clause 5(b) in the annex to the SCC Decision, that the legislation of the third country concerned does not allow him or her to comply with the standard data protection clauses in that annex, it follows from Clause 12 in that annex that data that has already been transferred to that third country and the copies thereof must be returned or destroyed in their entirety. In any event, under Clause 6 in that annex, breach of those standard clauses will result in a right for the person concerned to receive compensation for the damage suffered.  
144    It should be added that, under Clause 4(f) in the annex to the SCC Decision, a controller established in the European Union undertakes, where special categories of data could be transferred to a third country not providing adequate protection, to inform the data subject before, or as soon as possible after, the transfer. That notice enables the data subject to be in a position to bring legal action against the controller pursuant to Clause 3(1) in that annex so that the controller suspends the proposed transfer, terminates the contract concluded with the recipient of the personal data or, where appropriate, requires the recipient to return or destroy the data transferred.  
145    Lastly, under Clause 4(g) in that annex, the controller established in the European Union is required, when the recipient of personal data notifies him or her, pursuant to Clause 5(b), in the event of a change in the relevant legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the standard data protection clauses, to forward any notification to the competent supervisory authority if the controller established in the European Union decides, notwithstanding that notification, to continue the transfer or to lift the suspension. The forwarding of such a notification to that supervisory authority and its right to conduct an audit of the recipient of personal data pursuant to Clause 8(2) in that annex enable that supervisory authority to ascertain whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection.  
146    In that context, Article 4 of the SCC Decision, read in the light of recital 5 of Implementing Decision 2016/2297, supports the view that the SCC Decision does not prevent the competent supervisory authority from suspending or prohibiting, as appropriate, a transfer of personal data to a third country pursuant to the standard data protection clauses in the annex to that decision. In that regard, as is apparent from the answer to the eighth question, unless there is a valid Commission adequacy decision, the competent supervisory authority is required, under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such a transfer, if, in its view and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.  
147    As regards the fact, underlined by the Commissioner, that transfers of personal data to such a third country may result in the supervisory authorities in the various Member States adopting divergent decisions, it should be added that, as is clear from Article 55(1) and Article 57(1)(a) of the GDPR, the task of enforcing that regulation is conferred, in principle, on each supervisory authority on the territory of its own Member State. Furthermore, in order to avoid divergent decisions, Article 64(2) of the GDPR provides for the possibility for a supervisory authority which considers that transfers of data to a third country must, in general, be prohibited, to refer the matter to the European Data Protection Board (EDPB) for an opinion, which may, under Article 65(1)(c) of the GDPR, adopt a binding decision, in particular where a supervisory authority does not follow the opinion issued.  
148    It follows that the SCC Decision provides for effective mechanisms which, in practice, ensure that the transfer to a third country of personal data pursuant to the standard data protection clauses in the annex to that decision is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them.  
149    In the light of all of the foregoing considerations, the answer to the 7th and 11th questions is that examination of the SCC Decision in the light of Articles 7, 8 and 47 of the Charter has disclosed nothing to affect the validity of that decision.  
   
The  
   
4th, 5th, 9th and 10th  
 questions  
150    By its ninth question, the referring court wishes to know, in essence, whether and to what extent findings in the Privacy Shield Decision to the effect that the United States ensures an adequate level of protection are binding on the supervisory authority of a Member State. By its 4th, 5th and 10th questions, that court asks, in essence, whether, in view of its own findings on US law, the transfer to that third country of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision breaches the rights enshrined in Articles 7, 8 and 47 of the Charter and asks the Court, in particular, whether the introduction of the ombudsperson referred to in Annex III to the Privacy Shield Decision is compatible with Article 47 of the Charter.  
151    As a preliminary matter, it should be noted that, although the Commissioner’s action in the main proceedings only calls into question the SCC Decision, that action was brought before the referring court prior to the adoption of the Privacy Shield Decision. In so far as, by its fourth and fifth questions, that court asks the Court, at a general level, what protection must be ensured, under Articles 7, 8 and 47 of the Charter, in the context of such a transfer, the Court’s analysis must take into consideration the consequences arising from the subsequent adoption of the Privacy Shield Decision. A fortiori that is the case in so far as the referring court asks expressly, by its 10th question, whether the protection required by Article 47 of the Charter is ensured by the offices of the ombudsperson to which the Privacy Shield Decision refers.  
152    In addition, it is clear from the information provided in the order for reference that, in the main proceedings, Facebook Ireland claims that the Privacy Shield Decision is binding on the Commissioner in respect of the finding on the adequacy of the level of protection ensured by the United States and therefore in respect of the lawfulness of a transfer to that third country of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision.  
153    As appears from paragraph 59 above, in its judgment of 3 October 2017, provided in an annex to the order for reference, the referring court stated that it was obliged to take account of amendments to the law that may have occurred in the interval between the institution of the proceedings and the hearing of the action before it. Thus, that court would appear to be obliged to take into account, in order to dispose of the case in the main proceedings, the change in circumstances brought about by the adoption of the Privacy Shield Decision and any binding force it may have.  
154    In particular, the question whether the finding in the Privacy Shield Decision that the United States ensures an adequate level of protection is binding is relevant for the purposes of assessing both the obligations, set out in paragraphs 141 and 142 above, of the controller and recipient of personal data transferred to a third country pursuant to the standard data protection clauses in the annex to the SCC Decision and also any obligations to which the supervisory authority may be subject to suspend or prohibit such a transfer.  
155    As to whether the Privacy Shield Decision has binding effects, Article 1(1) of that decision provides that, for the purposes of Article 45(1) of the GDPR, ‘the United States ensures an adequate level of protection for personal data transferred from the [European] Union to organisations in the United States under the EU-U.S. Privacy Shield’. In accordance with Article 1(3) of the decision, personal data are regarded as transferred under the EU-US Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the ‘Privacy Shield List’, maintained and made publicly available by the US Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II to that decision.  
156    As follows from the case-law set out in paragraphs 117 and 118 above, the Privacy Shield Decision is binding on the supervisory authorities in so far as it finds that the United States ensures an adequate level of protection and, therefore, has the effect of authorising personal data transferred under the EU-US Privacy Shield. Therefore, until the Court should declare that decision invalid, the competent supervisory authority cannot suspend or prohibit a transfer of personal data to an organisation that abides by that privacy shield on the ground that it considers, contrary to the finding made by the Commission in that decision, that the US legislation governing the access to personal data transferred under that privacy shield and the use of that data by the public authorities of that third country for national security, law enforcement and other public interest purposes does not ensure an adequate level of protection.  
157    The fact remains that, in accordance with the case-law set out in paragraphs 119 and 120 above, when a person lodges a complaint with the competent supervisory authority, that authority must examine, with complete independence, whether the transfer of personal data at issue complies with the requirements laid down by the GDPR and, if, in its view, the arguments put forward by that person with a view to challenging the validity of an adequacy decision are well founded, bring an action before the national courts in order for them to make a reference to the Court for a preliminary ruling for the purpose of examining the validity of that decision.  
158    A complaint lodged under Article 77(1) of the GDPR, by which a person whose personal data has been or could be transferred to a third country contends that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 45(3) of the GDPR, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, the issue of whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals (see, by analogy, as regards Article 25(6) and Article 28(4) of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 59).  
159    In the present case, in essence, Mr Schrems requested the Commissioner to prohibit or suspend the transfer by Facebook Ireland of his personal data to Facebook Inc., established in the United States, on the ground that that third country did not ensure an adequate level of protection. Following an investigation into Mr Schrems’s claims, the Commissioner brought the matter before the referring court and that court appears, in the light of the evidence adduced and of the competing arguments put by the parties before it, to be unsure whether Mr Schrems’s doubts as to the adequacy of the level of protection ensured in that third country are well founded, despite the subsequent findings of the Commission in the Privacy Shield Decision, and that has led that court to refer the 4th, 5th and 10th questions to the Court for a preliminary ruling.  
160    As the Advocate General observed in point 175 of his Opinion, those questions must therefore be regarded, in essence, as calling into question the Commission’s finding, in the Privacy Shield Decision, that the United States ensures an adequate level of protection of personal data transferred from the European Union to that third country, and, therefore, as calling into question the validity of that decision.  
161    In the light of the considerations set out in paragraphs 121 and 157 to 160 above and in order to give the referring court a full answer, it should therefore be examined whether the Privacy Shield Decision complies with the requirements stemming from the GDPR read in the light of the Charter (see, by analogy, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 67).  
162    In order for the Commission to adopt an adequacy decision pursuant to Article 45(3) of the GDPR, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 96).  
   
The Privacy Shield Decision  
163    The Commission found, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-US Privacy Shield, the latter being comprised, inter alia, under Article 1(2) of that decision, of the Principles issued by the US Department of Commerce on 7 July 2016 as set out in Annex II to the decision and the official representations and commitments contained in the documents listed in Annexes I and III to VII to that decision.  
164    However, the Privacy Shield Decision also states, in paragraph I.5. of Annex II, under the heading ‘EU-U.S. Privacy Shield Framework Principles’, that adherence to those principles may be limited, inter alia, ‘to the extent necessary to meet national security, public interest, or law enforcement requirements’. Thus, that decision lays down, as did Decision 2000/520, that those requirements have primacy over those principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard the principles without limitation where they conflict with the requirements and therefore prove incompatible with them (see, by analogy, as regards Decision 2000/520, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 86).  
165    In the light of its general nature, the derogation set out in paragraph I.5 of Annex II to the Privacy Shield Decision thus enables interference, based on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States (see, by analogy, as regards Decision 2000/520, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 87). More particularly, as noted in the Privacy Shield Decision, such interference can arise from access to, and use of, personal data transferred from the European Union to the United States by US public authorities through the PRISM and UPSTREAM surveillance programmes under Section 702 of the FISA and E.O. 12333.  
166    In that context, in recitals 67 to 135 of the Privacy Shield Decision, the Commission assessed the limitations and safeguards available in US law, inter alia under Section 702 of the FISA, E.O. 12333 and PPD-28, as regards access to, and use of, personal data transferred under the EU-US Privacy Shield by US public authorities for national security, law enforcement and other public interest purposes.  
167    Following that assessment, the Commission found, in recital 136 of that decision, that ‘the United States ensures an adequate level of protection for personal data transferred from the [European] Union to self-certified organisations in the United States’, and, in recital 140 of the decision, it considered that, ‘on the basis of the available information about the U.S. legal order, … any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the [European] Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference’.  
   
The finding of an adequate level of protection  
168    In the light of the factors mentioned by the Commission in the Privacy Shield Decision and the referring court’s findings in the main proceedings, the referring court harbours doubts as to whether US law in fact ensures the adequate level of protection required under Article 45 of the GDPR, read in the light of the fundamental rights guaranteed in Articles 7, 8 and 47 of the Charter. In particular, that court considers that the law of that third country does not provide for the necessary limitations and safeguards with regard to the interferences authorised by its national legislation and does not ensure effective judicial protection against such interferences. As far as concerns effective judicial protection, it adds that the introduction of a Privacy Shield Ombudsperson cannot, in its view, remedy those deficiencies since an ombudsperson cannot be regarded as a tribunal within the meaning of Article 47 of the Charter.  
169    As regards, in the first place, Articles 7 and 8 of the Charter, which contribute to the level of protection required within the European Union, compliance with which must be established by the Commission before it adopts an adequacy decision under Article 45(1) of the GDPR, it must be borne in mind that Article 7 of the Charter states that everyone has the right to respect for his or her private and family life, home and communications. Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her.  
170    Thus, access to a natural person’s personal data with a view to its retention or use affects the fundamental right to respect for private life guaranteed in Article 7 of the Charter, which concerns any information relating to an identified or identifiable individual. Such processing of data also falls within the scope of Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article (see, to that effect, judgments of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 49 and 52, and of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 29; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 122 and 123).  
171    The Court has held that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (see, to that effect, judgments of 20 May 2003,   
Österreichischer Rundfunk and Others  
, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraphs 74 and 75, and of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 33 to 36; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126).  
172    However, the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgments of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48 and the case-law cited, and of 17 October 2013,   
Schwarz  
, C-291/12, EU:C:2013:670, paragraph 33 and the case-law cited; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 136).  
173    In this connection, it should also be observed that, under Article 8(2) of the Charter, personal data must, inter alia, be processed ‘for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.  
174    Furthermore, in accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.  
175    Following from the previous point, it should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 139 and the case-law cited).  
176    Lastly, in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 140 and 141 and the case-law cited).  
177    To that effect, Article 45(2)(a) of the GDPR states that, in its assessment of the adequacy of the level of protection in a third country, the Commission is, in particular, to take account of ‘effective and enforceable data subject rights’ for data subjects whose personal data are transferred.  
178    In the present case, the Commission’s finding in the Privacy Shield Decision that the United States ensures an adequate level of protection for personal data essentially equivalent to that guaranteed in the European Union by the GDPR, read in the light of Articles 7 and 8 of the Charter, has been called into question, inter alia, on the ground that the interference arising from the surveillance programmes based on Section 702 of the FISA and on E.O. 12333 are not covered by requirements ensuring, subject to the principle of proportionality, a level of protection essentially equivalent to that guaranteed by the second sentence of Article 52(1) of the Charter. It is therefore necessary to examine whether the implementation of those surveillance programmes is subject to such requirements, and it is not necessary to ascertain beforehand whether that third country has complied with conditions essentially equivalent to those laid down in the first sentence of Article 52(1) of the Charter.  
179    In that regard, as regards the surveillance programmes based on Section 702 of the FISA, the Commission found, in recital 109 of the Privacy Shield Decision, that, according to that article, ‘the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI)’. As is clear from that recital, the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether ‘individuals are properly targeted to acquire foreign intelligence information’.  
180    It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances and as the Advocate General stated, in essence, in points 291, 292 and 297 of his Opinion, that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter, as interpreted by the case-law set out in paragraphs 175 and 176 above, according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.  
181    According to the findings in the Privacy Shield Decision, the implementation of the surveillance programmes based on Section 702 of the FISA is, indeed, subject to the requirements of PPD-28. However, although the Commission stated, in recitals 69 and 77 of the Privacy Shield Decision, that such requirements are binding on the US intelligence authorities, the US Government has accepted, in reply to a question put by the Court, that PPD-28 does not grant data subjects actionable rights before the courts against the US authorities. Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights.  
182    As regards the monitoring programmes based on E.O. 12333, it is clear from the file before the Court that that order does not confer rights which are enforceable against the US authorities in the courts either.  
183    It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for ‘“bulk” collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection’, as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.  
184    It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.  
185    In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.  
186    In the second place, as regards Article 47 of the Charter, which also contributes to the required level of protection in the European Union, compliance with which must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of the GDPR, it should be noted that the first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled to a hearing by an independent and impartial tribunal.  
187    According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter (judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 95 and the case-law cited).  
188    To that effect, Article 45(2)(a) of the GDPR requires the Commission, in its assessment of the adequacy of the level of protection in a third country, to take account, in particular, of ‘effective administrative and judicial redress for the data subjects whose personal data are being transferred’. Recital 104 of the GDPR states, in that regard, that the third country ‘should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States’ data protection authorities’, and adds that ‘the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress’.  
189    The existence of such effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since, as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects’ complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country.  
190    In the present case, the Commission’s finding in the Privacy Shield Decision that the United States ensures a level of protection essentially equivalent to that guaranteed in Article 47 of the Charter has been called into question on the ground, inter alia, that the introduction of a Privacy Shield Ombudsperson cannot remedy the deficiencies which the Commission itself found in connection with the judicial protection of persons whose personal data is transferred to that third country.  
191    In that regard, the Commission found, in recital 115 of the Privacy Shield Decision, that ‘while individuals, including EU data subjects, … have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered’. Thus, as regards E.O. 12333, the Commission emphasised, in recital 115, the lack of any redress mechanism. In accordance with the case-law set out in paragraph 187 above, the existence of such a lacuna in judicial protection in respect of interferences with intelligence programmes based on that presidential decree makes it impossible to conclude, as the Commission did in the Privacy Shield Decision, that United States law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.  
192    Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy.  
193    The Commission found, however, in recitals 115 and 116 of the Privacy Shield Decision, that, as a result of the Ombudsperson Mechanism introduced by the US authorities, as described in a letter from the US Secretary of State to the European Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, set out in Annex III to that decision, and of the nature of that Ombudsperson’s role, in the present instance, a ‘Senior Coordinator for International Information Technology Diplomacy’, the United States can be deemed to ensure a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.  
194    An examination of whether the ombudsperson mechanism which is the subject of the Privacy Shield Decision is in fact capable of addressing the Commission’s finding of limitations on the right to judicial protection must, in accordance with the requirements arising from Article 47 of the Charter and the case-law recalled in paragraph 187 above, start from the premiss that data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data.  
195    In the letter referred to in paragraph 193 above, the Privacy Shield Ombudsperson, although described as ‘independent from the Intelligence Community’, was presented as ‘[reporting] directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided’. Furthermore, in addition to the fact that, as found by the Commission in recital 116 of that decision, the Ombudsperson is appointed by the Secretary of State and is an integral part of the US State Department, there is, as the Advocate General stated in point 337 of his Opinion, nothing in that decision to indicate that the dismissal or revocation of the appointment of the Ombudsperson is accompanied by any particular guarantees, which is such as to undermine the Ombudsman’s independence from the executive (see, to that effect, judgment of 21 January 2020,   
Banco de Santander  
, C-274/14, EU:C:2020:17, paragraphs 60 and 63 and the case-law cited).  
196    Similarly, as the Advocate General stated, in point 338 of his Opinion, although recital 120 of the Privacy Shield Decision refers to a commitment from the US Government that the relevant component of the intelligence services is required to correct any violation of the applicable rules detected by the Privacy Shield Ombudsperson, there is nothing in that decision to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely.  
197    Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.  
198    Therefore, in finding, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in that third country under the EU-US Privacy Shield, the Commission disregarded the requirements of Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter.  
199    It follows that Article 1 of the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.  
200    Since Article 1 of the Privacy Shield Decision is inseparable from Articles 2 and 6 of, and the annexes to, that decision, its invalidity affects the validity of the decision in its entirety.  
201    In the light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid.  
202    As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum (see, to that effect, judgment of 28 April 2016,   
Borealis Polyolefine and Others  
, C-191/14, C-192/14, C-295/14, C-389/14 and C-391/14 to C-393/14, EU:C:2016:311, paragraph 106), the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.  
   
Costs  
203    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 2(1) and (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that that regulation applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.  
2.        
Article 46(1) and Article 46(2)(c) of Regulation 2016/679 must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.  
3.        
Article 58(2)(f) and (j) of Regulation 2016/679 must be interpreted as meaning that, unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the Charter of Fundamental Rights, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.  
4.        
Examination of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EU of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision.  
5.        
Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid.  
Lenaerts  
Silva de Lapuerta  
Arabadjiev  
Prechal  
Vilaras  
Safjan  
Rodin  
Xuereb  
Rossi  
Jarukaitis  
Ilešič  
von Danwitz  
   
      Šváby        
   
Delivered in open court in Luxembourg on 16 July 2020.  
A. Calot Escobar  
   
K. Lenaerts  
Registrar  
   
President  
\*      Language of the case: English.  
   
  
  
  
  
Disclaimer

ID: 1ad6b43e-cc72-44be-b1a6-e7f37b3a2149

of 24 Feb 2022, C-175/20 (  
Valsts ieņēmumu dienests  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness, fairness and transparency   
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accuracy   
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Integrity and confidentiality   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
   
Judgment of the Court (Fifth Chamber) of 24 February 2022 (request for a preliminary ruling from the Administratīvā apgabaltiesa – Latvia) – ‘SS’ SIA v Valsts ieņēmumu dienests  
(Case C-175/20) 1  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 2 – Scope – Article 4 – Concept of ‘processing’ – Article 5 – Principles relating to processing – Purpose limitation – Data minimisation – Article 6 – Lawfulness of processing – Processing necessary for the performance of a task carried out in the public interest by the controller – Processing necessary for compliance with a legal obligation to which the controller is subject – Article 23 – Limitations – Processing of data for tax purposes – Request for the disclosure of information relating to vehicle sale advertisements placed online – Proportionality)  
Language of the case: Latvian  
Referring court  
Administratīvā apgabaltiesa  
Parties to the main proceedings  
Applicant:  
 ‘SS’ SIA  
Defendant:  
 Valsts ieņēmumu dienests  
Operative part of the judgment  
1.    The provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as meaning that the collection by the tax authorities of a Member State from an economic operator of information involving a significant amount of personal data is subject to the requirements of that regulation, in particular those set out in Article 5(1) thereof.  
2.    The provisions of Regulation 2016/679 must be interpreted as meaning that the tax authorities of a Member State may not derogate from the provisions of Article 5(1) of that regulation where such a right has not been granted to them by a legislative measure within the meaning of Article 23(1) thereof.  
3.    The provisions of Regulation 2016/679 must be interpreted as not precluding the tax authorities of a Member State from requiring a provider of internet advertisement services to disclose to them information relating to taxpayers who have published advertisements in one of the sections of their internet portal, provided, in particular, that those data are necessary in the light of the specific purposes for which they are collected and that the period to which the data collection relates does not exceed the period strictly necessary to achieve the objective of general interest sought.  
\_\_\_\_\_\_\_\_\_\_\_\_  
1 OJ C 222, 6.7.2020.  
   
  
  
  
  
Disclaimer

ID: 2a045665-0816-4031-a2a5-205355c96a52

Judgment of 9 Nov 2023, C-319/22 (  
Scania  
)  
   
JUDGMENT OF THE COURT (Third Chamber)  
9 November 2023 (\*)  
(Reference for a preliminary ruling – Market for motor vehicle repair and maintenance information services – Regulation (EU) 2018/858 – Approval and market surveillance of repair and maintenance information services for motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles – Article 61(1) and (2) – Annex X, point 6.1 – Independent operators – Information ‘easily accessible in the form of machine-readable and electronically readable data sets’ – Regulation (EU) 2016/679 – Article 6(1)(c) – Processing of personal data – Legal obligation on car manufacturers to make vehicle identification numbers (VIN) available to independent operators)  
In Case C-319/22,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Landgericht Köln (Regional Court, Cologne, Germany), made by decision of 4 May 2022, received at the Court on 11 May 2022, in the proceedings  
Gesamtverband Autoteile-Handel eV  
v  
Scania CV AB,  
THE COURT (Third Chamber),  
composed of K. Jürimäe, President of the Chamber, N. Piçarra (Rapporteur), M. Safjan, N. Jääskinen and M. Gavalec, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        Gesamtverband Autoteile-Handel eV, by E. Macher, M. Sacré and P. Schmitz, Rechtsanwälte,  
–        Scania CV AB, by F. Hübener, B. Lutz and D. Wendel, Rechtsanwälte,  
–        the European Commission, by A. Bouchagiar, M. Huttunen and M. Noll-Ehlers, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 4 May 2023,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 61(1) and (2) of Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ 2018 L 151, p. 1), and Article 6(1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
2        The request has been made in proceedings between Gesamtverband Autoteile-Handel eV (‘Gesamtverband’), a German trade association representing wholesalers of motor vehicle parts, and Scania CV AB (‘Scania’), a Swedish vehicle manufacturer, concerning Scania’s provision of vehicle on-board diagnostic (OBD) information and vehicle repair and maintenance information.  
   
Legal context  
   
Regulation 2018/858  
3        Recitals 50 and 62 of Regulation 2018/858 state:  
‘(50)      ‘Unrestricted access to vehicle repair and maintenance information, via a standardised format that can be used to retrieve the technical information, and effective competition in the market for services providing such information, are necessary to improve the functioning of the internal market, in particular as regards the free movement of goods, the freedom of establishment and the freedom to provide services. …  
…  
(52)      In order to ensure effective competition in the market for vehicle repair and maintenance information services, and in order to clarify that the information concerned also covers information which needs to be provided to independent operators other than repairers, so as to ensure that the independent vehicle repair and maintenance market as a whole can compete with authorised dealers … it is necessary to set out the details of the information to be provided for the purposes of access to vehicle repair and maintenance information.  
…  
(62)      Whenever the measures provided for in this Regulation entail the processing of personal data, they should be carried out in accordance with [the GDPR] …’  
4        Points (40), (45), (48) and (49) of Article 3 of Regulation 2018/858 are worded as follows:  
‘For the purposes of this Regulation and the regulatory acts listed in Annex II, except as otherwise provided therein, the following definitions apply:  
…  
40.      “manufacturer” means a natural or legal person who is responsible for all aspects of the type-approval of a vehicle, system, component or separate technical unit, or the individual vehicle approval, or the authorisation process for parts and equipment, for ensuring conformity of production and for market surveillance matters regarding that vehicle, system, component, separate technical unit, part and equipment produced, irrespective of whether or not that person is directly involved in all stages of the design and construction of that vehicle, system, component or separate technical unit concerned;  
…  
45.      “independent operator” means a natural or legal person, other than an authorised dealer or repairer, who is directly or indirectly involved in the repair and maintenance of vehicles, and include repairers, manufacturers or distributors of repair equipment, tools or spare parts, as well as publishers of technical information, automobile clubs, roadside assistance operators, operators offering inspection and testing services, operators offering training for installers, manufacturers and repairers of equipment for alternative-fuel vehicles; it also means authorised repairers, dealers and distributors within the distribution system of a given vehicle manufacturer to the extent that they provide repair and maintenance services for vehicles in respect of which they are not members of the vehicle manufacturer’s distribution system;  
…  
48.      “vehicle repair and maintenance information” means all information, including all subsequent amendments and supplements thereto, that is required for diagnosing, servicing and inspecting a vehicle, preparing it for road worthiness testing, repairing, re-programming or re-initialising of a vehicle, or that is required for the remote diagnostic support of a vehicle or for the fitting on a vehicle of parts and equipment, and that is provided by the manufacturer to his authorised partners, dealers and repairers or is used by the manufacturer for the repair and maintenance purposes;  
49.      “vehicle [OBD] information” means the information generated by a system that is on board a vehicle or that is connected to an engine, and that is capable of detecting a malfunction, and, where applicable, is capable of signalling its occurrence by means of an alert system, is capable of identifying the likely area of malfunction by means of information stored in a computer memory, and is capable of communicating that information off-board.’  
5        Article 61 of that regulation, entitled ‘Manufacturers’ obligations to provide vehicle OBD information and vehicle repair and maintenance information’, provides:  
‘1.      Manufacturers shall provide to independent operators unrestricted, standardised and non-discriminatory access to vehicle OBD information, diagnostic and other equipment, tools including the complete references, and available downloads, of the applicable software and vehicle repair and maintenance information. Information shall be presented in an easily accessible manner in the form of machine-readable and electronically processable datasets. …  
…  
2.      Until the [European] Commission has adopted a relevant standard through the work of the European Committee for Standardisation (CEN) or a comparable standardisation body, the vehicle OBD information and vehicle repair and maintenance information shall be presented in an easily accessible manner that can be processed with reasonable effort by independent operators.  
The vehicle OBD information and the vehicle repair and maintenance information shall be made available on the websites of manufacturers using a standardised format or, if this is not feasible, due to the nature of the information, in another appropriate format. For independent operators other than repairers, the information shall also be given in a machine-readable format that is capable of being electronically processed with commonly available information technology tools and software and which allows independent operators to carry out the task associated with their business in the aftermarket supply chain.  
…  
4.      The details of the technical requirements for access to vehicle OBD information and vehicle repair and maintenance information, in particular technical specifications on how vehicle OBD information and vehicle repair and maintenance information are to be provided, are laid down in Annex X.  
…’  
6        Under point 2.5.1 of Annex X to that regulation, entitled ‘Access to vehicle OBD information and vehicle repair and maintenance information’, that information includes ‘an unequivocal identification of the vehicle, system, component or separate technical unit for which the manufacturer is responsible’.  
7        As set out in the third and fourth paragraphs of point 6.1 of that annex:  
‘Information on all parts of the vehicle, with which the vehicle, as identified by the [vehicle identification number (VIN)] and any additional criteria such as wheelbase, engine output, trim level or options, is equipped by the vehicle manufacturer and that can be replaced by spare parts offered by the vehicle manufacturer to its authorised repairers or dealers or third parties by means of reference to original equipment (OE) parts number, shall be made available, in the form of machine readable and electronically processable datasets, in a database that is easily accessible to independent operators.  
This database shall comprise the VIN, OE parts numbers, OE naming of the parts, validity attributes (valid-from and valid-to dates), fitting attributes and, where applicable, structuring characteristics.’  
   
Regulation (EU)   
No 1  
9/2011  
8        Article 2(2) of Commission Regulation (EU) No 19/2011 of 11 January 2011 concerning type-approval requirements for the manufacturer’s statutory plate and for the vehicle identification number of motor vehicles and their trailers and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ 2011 L 8, p. 1), which was repealed with effect from 5 July 2022, but remains applicable   
ratione temporis  
 to the dispute in the main proceedings, provided:  
‘For the purposes of this Regulation:  
…  
(2)      “vehicle identification number” (VIN) means the alphanumeric code assigned to a vehicle by the manufacturer in order to ensure proper identification of every vehicle’.  
9        Annex I to Regulation No 19/2011, entitled ‘Technical requirements’, contained Part B, point 1.2 of which provided that ‘the VIN shall be unique and unequivocally attributed to a specified vehicle’.  
   
The GDPR  
10      Article 2 of the GDPR, entitled ‘Material scope’, provides, in paragraph 1 thereof:  
‘This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.’  
11      Article 4 of that regulation is worded as follows:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person …; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …  
…’  
12      Article 6 of that regulation, entitled ‘Lawfulness of processing’, provides:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
…  
3.      The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.  
The purpose of the processing shall be defined in that legal basis … . The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.  
…’  
   
Directive 1999/37  
13      Point II.5 of Annex I to Council Directive 1999/37/EC of 29 April 1999 on the registration documents for vehicles (OJ 1999 L 138, p. 57), as amended by Commission Directive 2003/127/EC of 23 December 2003 (OJ 2004 L 10, p. 29), states that the registration certificate of a vehicle must contain the VIN, the name and address of the holder of that certificate, preceded by harmonised Community codes E and C.  
14      In accordance with point II.5 and point II.6 of that annex, a natural person may be designated in that certificate as owner of the vehicle (codes C.2 and C.4) or as a person who can use the vehicle by virtue of a legal right other than that of ownership (code C.3).  
   
Directive (EU) 2019/1024  
15      Recital 35 of Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and re-use of public sector information (OJ 2019 L 172, p. 56), states:  
‘A document should be considered to be in a machine-readable format if it is in a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it. …’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
16      Scania, which is one of the largest manufacturers of heavy goods vehicles in Europe and a ‘manufacturer’, within the meaning of point 40 of Article 3 of Regulation 2018/858, grants independent operators manual access to vehicle, repair and maintenance information on those vehicles and on the OBD system via a website. That website enables searches to be carried out either on the basis of general vehicle information, such as the model, engine or the year of manufacture, or on a given vehicle, by entering the last seven figures of the VIN of that vehicle. The results of those searches can only be printed or saved on the computer as a PDF file, which excludes automated use of data. The results of searches concerning information on spare parts can be saved in the form of an XML file.  
17      It is apparent from the order for reference that Scania does not make the VINs available to independent operators. Only repairers have access to those data, by virtue of the registration documents or the indication on the chassis of the vehicle entrusted by the customer for the maintenance or repair of the vehicle.  
18      Gesamtverband, together with its members, accounts for 80% of the turnover in the independent trade in motor vehicle parts in Germany. Taking the view that the access to information granted by Scania falls short of the requirements imposed on it by Article 61(1) and (2) of Regulation 2018/858, it requested the Landgericht Köln (Regional Court, Cologne, Germany), the referring court, to order Scania to grant independent operators other than repairers, referred to in point 45 of Article 3 of that regulation, access to vehicle repair and maintenance information, within the meaning of point 48 of Article 3 of that regulation, through a database interface, enabling automated queries to be carried out and the results to be downloaded in the form of sets of data intended for electronic use.  
19      The referring court considers that the outcome of the dispute before it depends on the interpretation of Article 61(1) and (2) of Regulation 2018/858. It asks, in the first place, whether the obligation imposed by paragraph 1 on vehicle manufacturers to present the information in an ‘easily accessible manner in the form of machine-readable and electronically processable datasets’ covers all vehicle repair and maintenance information, within the meaning of point 48 of Article 3 of that regulation, or only the information relating to spare parts, referred to in the third subparagraph of point 6.1 of Annex X to that regulation, to which Article 61(4) of that regulation refers.  
20      In the second place, the referring court notes that, although Article 61(1) and (2) of Regulation 2018/858 does not expressly require the vehicle manufacturer to establish a database interface, they nevertheless require that the information be presented in an ‘easily accessible’ manner. According to that court, manual consultation of that information, which it considers to be a time-consuming method of access, does not comply with that requirement.  
21      In the third place, the referring court asks whether Article 61(1) and (2) of Regulation 2018/858 must be interpreted as allowing a vehicle manufacturer to limit access, in relation to vehicle repair and maintenance information, to targeted searches by means of the VIN, without, however, making available to independent operators an up-to-date list of all the VINs of its vehicles.  
22      In the fourth place, the referring court notes that Article 61(1) of Regulation 2018/858, in so far as it requires independent operators to be provided with the information which it sets out in the form of ‘machine-readable and electronically processable datasets’, does not mean that the file format may be processed directly electronically, without an intermediate step such as conversion into another file format. It doubts, however, whether the tables and texts of a PDF file can be regarded as complying with Directive 2019/1024, recital 35 of which states that, in order for a document to be regarded as being in machine-readable format, it must be in a structured file format, so that software applications can easily identify and recognise specific data and extract them.  
23      In the fifth place, the referring court, while taking the view that, as a general rule, the VIN does not constitute personal data, questions whether Article 61 of Regulation 2018/858 must be interpreted as imposing on vehicle manufacturers a legal obligation to process data, within the meaning of Article 6(1)(c) of the GDPR.  
24      In those circumstances, the Landgericht Köln (Regional Court, Cologne) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Does the requirement laid down in the second sentence of Article 61(1) of [Regulation 2018/858] … cover all vehicle repair and maintenance information within the meaning of point 48 of Article 3 of that regulation, or is that requirement limited to ‘spare parts information’ … referred to in point 6.1 of Annex X to that regulation?  
(2)      Must the second sentence of Article 61(1) [and (2), second subparagraph, of Regulation No 2018/858] be interpreted as meaning that the vehicle manufacturer fulfils its obligations in that regard only by:  
(a)      making the information accessible via the internet by means of a machine-controlled query via a database interface, which provides the possibility to download the results, or is it sufficient that the vehicle manufacturer enables only a manual search by a human user on-screen on a website and limits the result of the query to the visible content of the pages displayed on-screen?  
and  
(b)      making it possible for all information in the database linked to the vehicle manufacturer’s vehicle identification numbers (VINs) to be searched for on the basis of those VINs, which are to be provided by it in a separate list, and, independently of that possibility,  
–        also on the basis of other vehicle identification characteristics in accordance with the third subparagraph of point 6.1 of Annex X to [Regulation 2018/858]  
–        and on the basis of the terms that the vehicle manufacturer otherwise uses for categories (such as categories of components, spare parts, repair and maintenance instructions and technical illustrations) and other database entries in any combination  
or is it sufficient that the manufacturer offers the search exclusively as an individual query based on the VIN of a single, specific vehicle without at the same time providing an up-to-date list of all its vehicles’ VINs?  
and  
(c)      providing those datasets in files in a format which is intended to make the datasets contained therein directly amenable to (further) electronic processing, the description of the dataset concerned being specified (in the case of texts and tables), or is the possibility to export mere screenshots in any conventional file format, such as a PDF file, sufficient for that purpose?  
(3)      Does Article 61(1) of Regulation [2018/858] constitute, for vehicle manufacturers, a legal obligation within the meaning of Article 6(1)(c) of the GDPR which justifies the disclosure of VINs or information linked to VINs to independent operators as other controllers within the meaning of point 7 of Article 4 of the GDPR?’  
   
Consideration of the questions referred  
   
The first question  
25      By its first question, the referring court asks, in essence, whether the second sentence of Article 61(1) of Regulation 2018/858 must be interpreted as meaning that the obligation to present the information referred to in that paragraph in an easily accessible manner, in the form of machine-readable and electronically processable data sets, covers all ‘vehicle repair and maintenance information’, within the meaning of point 48 of Article 3 of that regulation, or only the information relating to the spare parts referred to in point 6.1 of Annex X to that regulation.  
26      The first sentence of Article 61(1) of Regulation 2018/858 requires vehicle manufacturers to provide independent operators with unrestricted, standardised and non-discriminatory access, inter alia, to ‘vehicle repair and maintenance information’, within the meaning of point 48 of Article 3 of that regulation. Under the second sentence of Article 61(1) of that regulation, all such information must be presented in an easily accessible manner, in the form of machine-readable and electronically processable data sets.  
27      It thus follows from the wording itself of that provision that the obligation which it lays down covers the same information as that referred to in the first sentence of Article 61(1) of that regulation, namely, in particular, vehicle repair and maintenance information.  
28      Although, under Article 61(4) of Regulation 2018/858, ‘the details of the technical requirements for access … to vehicle repair and maintenance information, in particular technical specifications on how vehicle OBD information and vehicle repair and maintenance information are to be provided, are laid down in Annex X’, and although the third paragraph of point 6.1 of that annex refers only to information on vehicle parts which can be replaced by spare parts, the fact remains that the latter provision does not itself govern the extent of access to vehicle repair and maintenance information. It cannot therefore have the effect of reducing the vehicle repair and maintenance information to that relating to spare parts.  
29      In the light of the foregoing, the answer to the first question is that the second sentence of Article 61(1) of Regulation 2018/858 must be interpreted as meaning that the obligation to present the information referred to in that paragraph in an easily accessible manner, in the form of machine-readable and electronically processable datasets, covers all ‘vehicle repair and maintenance information’, within the meaning of   
   
point 48 of Article 3 of that regulation, and not only the information relating to spare parts referred to in point 6.1 of Annex X to that regulation.  
   
The second question  
30      By its second question, the referring court asks, in essence, whether the second sentence of Article 61(1) and the second subparagraph of Article 61(2) of Regulation 2018/858 must be interpreted as meaning that it requires vehicle manufacturers, first, to make vehicle repair and maintenance information accessible via a database interface enabling automated searches with downloading of results, second, to establish a database enabling search on the basis not only of the VIN but also of additional means and, third, to make that information available to independent operators in files the format of which allows the direct electronic use of the sets of data contained in those files.  
31      In the first place, as has been recalled in paragraph 26 of the present judgment, Article 61(1) of Regulation 2018/858 requires vehicle manufacturers to provide independent operators with unrestricted, standardised and non-discriminatory access, inter alia, to vehicle repair and maintenance information and to present it in a manner that is ‘easily accessible, in the form of machine-readable and electronically processable datasets’.  
32      The first sentence of the second subparagraph of Article 61(2) requires those manufacturers to make vehicle repair and maintenance information available on their websites in a standardised format or, if that is not feasible due to the nature of the information, in another appropriate format. The second sentence of that second subparagraph requires those manufacturers to provide that information to independent operators other than repairers in a machine-readable format, capable of being electronically processed by means of generally available computer tools and software, so that those operators can carry out their activities in the supply chain of the market for spare parts and equipment (see, to that effect, judgment of 27 October 2022,   
ADPA and Gesamtverband Autoteile-Handel  
, C-390/21, EU:C:2022:837, paragraph 28).  
33      Until the adoption by the Commission of an appropriate standard, the same manufacturers must, under the first subparagraph of Article 61(2) of Regulation 2018/858, present that information in an ‘easily accessible’ manner in such a way that it can be processed by independent operators ‘with reasonable effort’.  
34      However, Article 61 of that regulation does not impose an obligation on vehicle manufacturers to set up an interface that can be used to search those manufacturers’ databases.  
35      In the second place, under the third paragraph of point 6.1 of Annex X to Regulation 2018/858, to which Article 61(4) of that regulation refers, ‘information on all parts of the vehicle, with which the vehicle, as identified by the VIN and any additional criteria such as wheelbase, engine output, trim level or options, is equipped by the vehicle manufacturer and that can be replaced by spare parts offered by the vehicle manufacturer to its authorised repairers or dealers or third parties by means of reference to original equipment (OE) parts number, shall be made available, in the form of machine readable and electronically processable datasets, in a database that is easily accessible to independent operators’.  
36      It follows from the wording itself of the third paragraph of point 6.1 that, as regards information on parts that can be replaced by spare parts, manufacturers are required to create a database (see, to that effect, judgment of 19 September 2019,   
Gesamtverband Autoteile-Handel  
, C-527/18, EU:C:2019:762, paragraph 32), allowing searches to be carried out using not only the VIN but also the ‘additional criteria’ provided for in that provision.  
37      That interpretation is consistent with the objective of ensuring effective competition on the market for vehicle repair and maintenance information services, as set out in recitals 50 and 52 of Regulation 2018/858. To that end, independent operators, such as publishers of technical information and manufacturers of parts, must be able, in order to carry out their activities in the supply chain of the spare parts and equipment market, to carry out searches by all the means listed in the preceding paragraph of the present judgment.  
38      In the third place, the manufacturers’ obligation to make vehicle repair and maintenance information available to independent operators in a form amenable to electronic processing, laid down in Article 61(1) of Regulation 2018/858, must enable those operators to ‘retrieve the technical information’ (see, to that effect, judgment of 27 October 2022,   
ADPA and Gesamtverband Autoteile-Handel  
, C-390/21, EU:C:2022:837, paragraph 27).  
39      In addition, it should be noted that, according to recital 35 of Directive 2019/1024, in order for a document to be regarded as being in machine-readable format, it must be presented ‘in a file format structured in such a way that software applications can easily identify and recognise and extract specific data from it’.  
40      It is apparent from the order for reference that making information available in a format such as that offered by Scania lends itself only to indirect electronic processing and requires those operators to carry out intermediate stages of file conversion which do not allow automated processing in a directly processable format. Subject to the checks which it is ultimately for the referring court to carry out, such making available cannot be regarded as complying with the second sentence of Article 61(1) and the second subparagraph of Article 61(2) of Regulation 2018/858.  
41      That interpretation is consistent with the objective of ensuring effective competition on the market for vehicle repair and maintenance information services, as set out in recitals 50 and 52 of Regulation 2018/858. To that end, it is essential, as the Commission pointed out in its written observations, that independent operators should be able to extract technical data from the format by which manufacturers make the necessary information available to them and to retain those data immediately after their retrieval for re-use.  
42      In the light of the foregoing, the answer to the second question is that the second sentence of Article 61(1) and the second subparagraph of Article 61(2) of Regulation 2018/858 must be interpreted as meaning that:  
–        it does not require vehicle manufacturers to make vehicle repair and maintenance information accessible by means of a database interface allowing automated search with downloading of results, but requires them to make that information available to independent operators in files the format of which allows for direct electronic processing of the sets of data contained in those files;  
–        read in conjunction with Article 61(4) of that regulation and the third subparagraph of point 6.1 of Annex X thereto, it requires vehicle manufacturers to establish a database making it possible to search for information on all the original parts of the vehicle on the basis not only of the VIN but also of the additional means provided for in that provision.  
   
The third question  
43      By its third question, the referring court asks, in essence, whether Article 61(1) of Regulation 2018/858 must be interpreted as establishing a ‘legal obligation’, within the meaning of Article 6(1)(c) of the GDPR, on vehicle manufacturers, to make the VINs of the vehicles that they manufacture available to independent operators, as ‘controllers’, within the meaning of Article 4(7) of that regulation.  
44      In order to answer that question, it is necessary to examine, first, whether the VIN falls within the concept of ‘personal data’, within the meaning of Article 4(1) of the GDPR, which defines that concept as ‘any information relating to an identified or identifiable natural person’.  
45      That definition is applicable where, by reason of its content, purpose and effect, the information in question is linked to a particular natural person (judgment of 8 December 2022,   
Inspektor  
 v   
Inspektorata kam Visshia sadeben savet (Purposes of the processing of personal data – Criminal investigation)  
, C-180/21, EU:C:2022:967, paragraph 70). In order to determine whether a natural person is identifiable, directly or indirectly, account should be taken of all the means likely reasonably to be used either by the controller, within the meaning of Article 4(7) of the GDPR, or by any other person, to identify that person, without, however, requiring that all the information enabling that person to be identified should be in the hands of a single entity (see, to that effect, judgment of 19 October 2016,   
Breyer  
 (C-582/14, EU:C:2016:779, paragraphs 42 and 43).  
46      As the Advocate General observed in points 34 and 39 of his Opinion, a datum such as the VIN – which is defined by Article 2(2) of Regulation No 19/2011 as an alphanumeric code assigned to the vehicle by its manufacturer in order to ensure that the vehicle is properly identified and which, as such, is not ‘personal’ – becomes personal as regards someone who reasonably has means enabling that datum to be associated with a specific person.  
47      It follows from point II.5 of Annex I to Directive 1999/37 that the VIN must appear on the registration certificate for a vehicle, as must the name and address of the holder of that certificate. In addition, under points II.5 and II.6 of that annex, a natural person may be designated in that certificate as the owner of the vehicle, or as a person who can use the vehicle on a legal basis other than that of owner.  
48      In those circumstances, the VIN constitutes personal data, within the meaning of Article 4(1) of the GDPR, of the natural person referred to in that certificate, in so far as the person who has access to it may have means enabling him to use it to identify the owner of the vehicle to which it relates or the person who may use that vehicle on a legal basis other than that of owner.  
49      As the Advocate General observed in points 34 and 41 of his Opinion, where independent operators may reasonably have at their disposal the means enabling them to link a VIN to an identified or identifiable natural person, which it is for the referring court to determine, that VIN constitutes personal data for them, within the meaning of Article 4(1) of the GDPR, and, indirectly, for the vehicle manufacturers making it available, even if the VIN is not, in itself, personal data for them, and is not personal data for them in particular where the vehicle to which the VIN has been assigned does not belong to a natural person.  
50      If it follows from the determination referred to in the preceding paragraph of the present judgment that a VIN must be regarded as personal data, it falls within the scope of the GDPR, pursuant to Article 2(1) thereof, and must therefore be processed in accordance with that regulation.  
51      The concept of ‘processing’ is defined in Article 4(2) of the GDPR as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automatic means, such as disclosure by transmission, dissemination or otherwise making available. That concept therefore covers the making available of a VIN by the ‘controller’, within the meaning of Article 4(7) of that regulation, where that VIN makes it possible to identify a natural person.  
52      Article 6 of the GDPR lays down the conditions for the lawfulness of the processing of such data. In accordance with paragraph 1(c) of that article, processing is lawful where it is necessary for compliance with a legal obligation to which the controller is subject.  
53      Article 6(3) of the GDPR states, moreover, that that processing must be based on EU law or on Member State law to which the controller is subject and that that legal basis must define the purposes of the processing and meet a public interest objective, and be proportionate to the pursuit of such an objective.  
54      As stated in recital 62 of Regulation 2018/858, the rules on the protection of personal data must be applied whenever the measures provided for in that regulation entail the processing of personal data.  
55      It is in the light of the foregoing that it is necessary to examine, secondly, the content and scope of Article 61(1) of Regulation 2018/858.  
56      That provision, as has already been pointed out in paragraphs 26 and 31 of the present judgment, requires, first of all, vehicle manufacturers to make available to independent operators, inter alia, vehicle repair and maintenance information, defined in point 48 of Article 3 of that regulation as ‘all information, including all subsequent amendments and supplements thereto, that is required for diagnosing, servicing and inspecting a vehicle, preparing it for road worthiness testing, repairing, re-programming or re-initialising of a vehicle, or that is required for the remote diagnostic support of a vehicle or for the fitting on a vehicle of parts and equipment, and that is provided by the manufacturer to his authorised partners, dealers and repairers or is used by the manufacturer for the repair and maintenance purposes.’  
57      In addition, Annex X to Regulation 2018/858, to which Article 61(4) of that regulation refers, states, in point 2.5.1, that vehicle repair and maintenance information is to include ‘an unequivocal identification of the vehicle’. Furthermore, in accordance with the fourth paragraph of point 6.1 of that annex, the VIN is to appear in the database that the manufacturer is required to establish, pursuant to the third subparagraph of point 6.1, concerning the original parts of the vehicle that can be replaced by spare parts.  
58      Those provisions of EU law thus impose on vehicle manufacturers the ‘legal obligation’, within the meaning of Article 6(1)(c) of the GDPR, to make available to independent operators, among other data, the VINs. Such a ‘legal obligation’ satisfies the first condition for the lawfulness of the processing of personal data set out in paragraph 52 of the present judgment.  
59      Next, Article 61(1) of Regulation 2018/858 defines the purpose of that data processing obligation, which is to provide independent operators with unrestricted, standardised and non-discriminatory access to, inter alia, vehicle repair and maintenance information within the meaning of point 48 of Article 3 of that regulation. The ‘legal obligation’ for manufacturers to make the VINs of their vehicles available to independent operators therefore meets the objective, set out in recital 52 of that regulation, of ensuring effective and undistorted competition on the market for vehicle repair and maintenance information services.  
60      According to recital 50 of Regulation 2018/858, such competition is necessary in order to improve the functioning of the internal market, in particular as regards the free movement of goods, the freedom of establishment and the freedom to provide services. Therefore, the objective referred to in the preceding paragraph is in the public interest and, accordingly, legitimate (see, by analogy, judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 75). The second condition for the lawfulness of the processing of personal data set out in paragraph 53 of the present judgment is thus satisfied.  
61      As regards, lastly, the third condition for the lawfulness of the processing of personal data, laid down in Article 6(3) of the GDPR and requiring that that processing be ‘proportionate to the legitimate objective pursued’, it is sufficient to note, as the Advocate General did in the fourth indent of point 52 of his Opinion, first, that only the search using the VIN enables the data corresponding to a particular vehicle to be accurately identified and, second, that the file before the Court does not refer to any other less restrictive means of identification which, at the same time, would be as effective as search on the basis of the VIN and would enable the public interest objective identified in the preceding paragraph to be pursued. Article 61(1) of Regulation 2018/858 thus satisfies the third condition referred to in paragraph 53 of the present judgment.  
62      In the light of the foregoing, the answer to the third question is that Article 61(1) of Regulation 2018/858, read in conjunction with Article 61(4) and point 6.1 of Annex X to that regulation, must be interpreted as meaning that it establishes a ‘legal obligation’, within the meaning of Article 6(1)(c) of the GDPR, on car manufacturers, to make the VINs of the vehicles which they manufacture available to independent operators, as ‘controllers’, within the meaning of Article 4(7) of that regulation.  
   
Costs  
63      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
The second sentence of Article 61(1) of Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC,  
must be interpreted as meaning that the obligation to present the information referred to in that paragraph in an easily accessible manner, in the form of machine-readable and electronically processable datasets, covers all ‘vehicle repair and maintenance information’, within the meaning of point 48 of Article 3 of that regulation, and not only the information relating to spare parts referred to in point 6.1 of Annex X to that regulation.  
2.        
The second sentence of Article 61(1) and the second subparagraph of Article 61(2) of Regulation 2018/858  
must be interpreted as meaning that:  
–          
it does not require vehicle manufacturers to make vehicle repair and maintenance information accessible by means of a database interface allowing automated search with downloading of results, but requires them to make that information available to independent operators in files the format of which serves for direct electronic processing of the sets of data contained in those files;  
–          
read in conjunction with Article 61(4) of that regulation and the third subparagraph of point 6.1 of Annex X thereto, it requires vehicle manufacturers to establish a database making it possible to search for information on all the original parts of the vehicle on the basis not only of the vehicle identification number (VIN) but also of the additional means provided for in that provision.  
3.        
Article 61(1) of Regulation 2018/858, read in conjunction with Article 61(4) and with point 6.1 of Annex X to that regulation,  
must be interpreted as meaning that it establishes a ‘legal obligation’, within the meaning of Article 6(1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), on car manufacturers, to make the VINs of the vehicles which they manufacture available to independent operators, as ‘controllers’, within the meaning of Article 4(7) of that regulation.

ID: 2c0cf9c5-51a1-472e-b402-f6c187ea1476

of 21 Jun 2022, C-817/19 (  
Ligue des droits humains  
)  
   
JUDGMENT OF THE COURT (Grand Chamber)  
21 June 2022 (\*)  
Table of contents  
(Reference for a preliminary ruling – Processing of personal data – Passenger Name Records (PNR) – Regulation (EU) 2016/679 – Article 2(2)(d) – Scope – Directive (EU) 2016/681 – Use of PNR data of air passengers of flights operated between the European Union and third countries – Power to include data of air passengers of flights operated within the European Union – Automated processing of that data – Retention period – Fight against terrorist offences and serious crime – Validity – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 21 as well as Article 52(1) – National legislation extending the application of the PNR system to other transport operations within the European Union – Freedom of movement within the European Union – Charter of Fundamental Rights – Article 45)  
In Case C-817/19,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 17 October 2019, received at the Court on 31 October 2019, in the proceedings  
Ligue des droits humains  
v  
Conseil des ministres,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Arabadjiev, S. Rodin, I. Jarukaitis and N. Jääskinen, Presidents of Chambers, T. von Danwitz (Rapporteur), M. Safjan, F. Biltgen, P.G. Xuereb, N. Piçarra, L.S. Rossi, A. Kumin and N. Wahl, Judges,  
Advocate General: G. Pitruzzella,  
Registrar: M. Krausenböck, Administrator,  
having regard to the written procedure and further to the hearing on 13 July 2021,  
after considering the observations submitted on behalf of:  
–        the Ligue des droits humains, by C. Forget, avocate,  
–        the Belgian Government, by P. Cottin, J.-C. Halleux, C. Pochet, M. Van Regemorter, acting as Agents, and by C. Caillet, advocaat, E. Jacubowitz, avocat, G. Ceuppens, V. Dethy and D. Vertongen,  
–        the Czech Government, by T. Machovičová, O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
–        the Danish Government, by M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen and M. Søndahl Wolff, acting as Agents,  
–        the German Government, by D. Klebs and J. Möller, acting as Agents,  
–        the Estonian Government, by N. Grünberg, acting as Agent,  
–        Ireland, by M. Browne, A. Joyce, J. Quaney, acting as Agents, and D. Fennelly, Barrister-at-Law,  
–        the Spanish Government, by L. Aguilera Ruiz, acting as Agent,  
–        the French Government, by D. Dubois, E. de Moustier and T. Stéhelin, acting as Agents,  
–        the Cypriot Government, by I. Neofytou, acting as Agent,  
–        the Latvian Government, by E. Bārdiņš, K. Pommere and V. Soņeca, acting as Agents,  
–        the Netherlands Government, by M.K. Bulterman, A. Hanje, J. Langer and C.S. Schillemans, acting as Agents,  
–        the Austrian Government, by G. Kunnert, A. Posch and J. Schmoll, acting as Agents,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Slovak Government, by B. Ricziová, acting as Agent,  
–        the Finnish Government, by A. Laine and H. Leppo, acting as Agent,  
–        the European Parliament, by O. Hrstková Šolcová and P. López-Carceller, acting as Agents,  
–        the Council of the European Union, by J. Lotarski, N. Rouam, E. Sitbon and C. Zadra, acting as Agents,  
–        the European Commission, by D. Nardi and M. Wasmeier, acting as Agents,  
–        the European Data Protection Supervisor, by P. Angelov, A. Buchta, F. Coudert and C.-A. Marnier, acting as Agents,  
–        the European Union Agency for Fundamental Rights, by L. López, T. Molnar, M. Nespor and M. O’Flaherty, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 27 January 2022,  
gives the following  
Judgment  
1        This reference for a preliminary ruling, in essence, concerns:  
–        the interpretation of Article 2(2)(d) and Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’), of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ 2004 L 261, p. 24; ‘the API Directive’) and of Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC (OJ 2010 L 283, p. 1);  
–        the interpretation and validity, in the light of Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’), of Article 3(4) and Articles 6 and 12 of, as well as Annex I to, Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132; ‘the PNR Directive’), and   
–        the interpretation and validity, in the light of Article 3(2) TEU and Article 45 of the Charter, of the API Directive.  
2        The request has been made in proceedings between the Ligue des droits humains and the Conseil des ministres (Council of Ministers, Belgium) concerning the legality of the loi du 25 décembre 2016, relative au traitement des données des passagers (Law of 25 December 2016 on the processing of passenger data).  
I.        
Legal context  
A.        
European Union law  
1.        
Directive 95/46/EC  
3        Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) was repealed by the GDPR, with effect from 25 May 2018. Article 3(2) of that directive provided:  
‘This Directive shall not apply to the processing of personal data:  
–      in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–      by a natural person in the course of a purely personal or household activity.’  
2.        
The API Directive  
4        Recitals 1, 7, 9 and 12 of the API Directive state:  
‘(1)      In order to combat illegal immigration effectively and to improve border control, it is essential that all Member States introduce provisions laying down obligations on air carriers transporting passengers into the territory of the Member States. In addition, in order to ensure the greater effectiveness of this objective, the financial penalties currently provided for by the Member States for cases where carriers fail to meet their obligations should be harmonised to the extent possible, taking into account the differences in legal systems and practices between the Member States.  
…  
(7)      The obligations to be imposed on carriers by virtue of this Directive are complementary to those established pursuant to the provisions of Article 26 of the 1990 Schengen Convention implementing the Schengen Agreement of 14 June 1985, as supplemented by Council Directive 2001/51/EC [of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985 (OJ 2001 L 187, p. 45)], the two types of obligation serving the same objective of curbing migratory flows and combating illegal immigration.  
…  
(9)      In order to combat illegal immigration more effectively and in order to ensure the greater effectiveness of this objective, it is essential that, without prejudice to the provisions of Directive [95/46], account be taken at the earliest opportunity of any technological innovation, especially with reference to the integration and use of biometric features in the information to be provided by the carriers.  
…  
(12)      Directive [95/46] applies with regard to the processing of personal data by the authorities of the Member States. This means, that whereas it would be legitimate to process the passenger data transmitted for the performance of border checks also for the purposes of allowing their use as evidence in proceedings aiming at the enforcement of the laws and regulations on entry and immigration, including their provisions on the protection of public policy (  
ordre public  
) and national security, any further processing in a way incompatible with those purposes would run counter to the principle set out in Article 6(1)(b) of Directive [95/46]. Member States should provide for a system of sanctions to be applied in the event of use contrary to the purpose of the present Directive.’  
5        Article 1 of the API Directive, entitled ‘Objective’, provides:  
‘This Directive aims at improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities.’  
6        Article 2 of that directive, entitled ‘Definitions’, states:   
‘For the purpose of this Directive:  
(a)      “carrier” means any natural or legal person whose occupation it is to provide passenger transport by air;  
(b)      “external borders” means the external borders of the Member States with third countries;  
(c)      “border control” means a check carried out at a border in response exclusively to an intention to cross that border, regardless of any other consideration;  
(d)      “border crossing point” means any crossing point authorised by the competent authorities for crossing external borders;  
(e)      “personal data”, “processing of personal data” and “personal data filing system” have the meaning as stipulated under Article 2 of Directive [95/46].’  
7        Article 3 of that directive, entitled ‘Data transmission’, provides, in its paragraphs 1 and 2:  
‘1.      Member States shall take the necessary steps to establish an obligation for carriers to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State.  
2.      The information referred to above shall comprise:  
–        the number and type of travel document used,  
–        nationality,  
–        full names,  
–        the date of birth,  
–        the border crossing point of entry into the territory of the Member States,  
–        code of transport,  
–        departure and arrival time of the transportation,  
–        total number of passengers carried on that transport,  
–        the initial point of embarkation.’  
8        Article 6 of the API Directive, entitled ‘Data processing’, provides:  
‘1.      The personal data referred to in Article 3(1) shall be communicated to the authorities responsible for carrying out checks on persons at external borders through which the passenger will enter the territory of a Member State, for the purpose of facilitating the performance of such checks with the objective of combating illegal immigration more effectively.  
Member States shall ensure that these data are collected by the carriers and transmitted electronically or, in case of failure, by any other appropriate means to the authorities responsible for carrying out border checks at the authorised border crossing point through which the passenger will enter the territory of a Member State. The authorities responsible for carrying out checks on persons at external borders shall save the data in a temporary file.  
After passengers have entered, these authorities shall delete the data, within 24 hours after transmission, unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders in accordance with national law and subject to data protection provisions under Directive [95/46].  
Member States shall take the necessary measures to oblige carriers to delete, within 24 hours of the arrival of the means of transportation pursuant to Article 3(1), the personal data they have collected and transmitted to the border authorities for the purposes of this Directive.  
In accordance with their national law and subject to data protection provisions under Directive [95/46], Member States may also use the personal data referred to in Article 3(1) for law enforcement purposes.  
2.      Member States shall take the necessary measures to oblige the carriers to inform the passengers in accordance with the provisions laid down in Directive [95/46]. This shall also comprise the information referred to in Article 10(c) and Article 11(1)(c) of Directive [95/46].’  
3.        
Directive 2010/65  
9        Directive 2010/65 is to be repealed, pursuant to Article 25 of Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65 (OJ 2019 L 198, p. 64), from 15 August 2025.  
10      Recital 2 of that directive states:  
‘For the facilitation of maritime transport and in order to reduce the administrative burdens for shipping companies, the reporting formalities required by legal acts of the [European] Union and by Member States need to be simplified and harmonised to the greatest extent possible. …’  
11      Article 1 of that directive, entitled ‘Subject matter and scope’, provides, in its paragraphs 1 and 2:  
‘1.      The purpose of this Directive is to simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard and by rationalising reporting formalities.  
2.      This Directive shall apply to the reporting formalities applicable to maritime transport for ships arriving in and ships departing from ports situated in Member States.’  
12      Under Article 8 of that directive, entitled ‘Confidentiality’:  
‘1.      Member States shall, in accordance with the applicable legal acts of the [European] Union or national legislation, take the necessary measures to ensure the confidentiality of commercial and other confidential information exchanged in accordance with this Directive.  
2.      Member States shall take particular care to protect commercial data collected under this Directive. In respect of personal data, Member States shall ensure that they comply with Directive [95/46]. The [EU] institutions and bodies shall ensure that they comply with Regulation (EC) No 45/2001 [of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1)].’  
4.        
The GDPR  
13      Recital 19 of the GDPR states:  
‘The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific [EU] legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific [EU] legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council [of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89)]. Member States may entrust competent authorities within the meaning of [Directive 2016/680] with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of [EU] law, falls within the scope of this Regulation.  
…’  
14      Article 2 of that regulation, entitled ‘Material scope’, provides in its paragraphs 1 and 2:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of [EU] law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V [TEU];  
…  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
15      Article 4 of that regulation, entitled ‘Definitions’, provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person …;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…’  
16      Article 23 of the GDPR, entitled ‘Restrictions’, provides:  
‘1.      [EU] or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as in Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;  
…  
(h)      a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);  
…  
2.      In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:  
(a)      the purposes of the processing or categories of processing;  
(b)      the categories of personal data;  
(c)      the scope of the restrictions introduced;  
(d)      the safeguards to prevent abuse or unlawful access or transfer;  
(e)      the specification of the controller or categories of controllers;  
(f)      the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;  
(g)      the risks to the rights and freedoms of data subjects; and  
(h)      the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.’  
17      Article 94 of that regulation, entitled ‘Repeal of Directive [95/46]’ provides:  
‘1.      Directive [95/46] is repealed with effect from 25 May 2018.  
2.      References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.’  
5.        
Directive 2016/680  
18      Directive 2016/680, in accordance with Article 59 thereof, repealed and replaced Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350, p. 60), from 6 May 2018.  
19      Recitals 9 to 11 of Directive 2016/680 state:  
‘(9)      On that basis, [the GDPR] lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the [European] Union.  
(10)      In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and on the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields.  
(11)      It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, [the GDPR] applies. [The GDPR] therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of [the GDPR] remains unaffected for the processing of personal data by the processor outside the scope of this Directive.’  
20      Article 1 of that directive, entitled ‘Subject matter and objectives’, which corresponds, in essence, to Article 1 of Framework Decision 2008/977, provides, in its paragraph 1:  
‘This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
21      Under Article 3 of that directive, entitled ‘Definitions’:  
‘For the purposes of this Directive:  
…  
7.      “competent authority” means:  
(a)      any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or  
(b)      any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;  
…’  
6.        
The PNR Directive  
22      Recitals 4 to 12, 15, 19, 20, 22, 25, 27, 28, 33, 36 and 37 of the PNR Directive state:  
‘(4)      [The API Directive] regulates the transfer of advance passenger information (API) data by air carriers to the competent national authorities for the purpose of improving border controls and combating illegal immigration.  
(5)      The objectives of this Directive are, inter alia, to ensure security, to protect the life and safety of persons, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities.  
(6)      Effective use of PNR data, for example by comparing PNR data against various databases on persons and objects sought, is necessary to prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security, to gather evidence and, where relevant, to find associates of criminals and unravel criminal networks.  
(7)      Assessment of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment and who should be subject to further examination by the competent authorities. By using PNR data it is possible to address the threat of terrorist offences and serious crime from a different perspective than through the processing of other categories of personal data. However, to ensure that the processing of PNR data remains limited to what is necessary, the creation and application of assessment criteria should be limited to terrorist offences and serious crime for which the use of such criteria is relevant. Furthermore, the assessment criteria should be defined in a manner which keeps to a minimum the number of innocent people wrongly identified by the system.  
(8)      Air carriers already collect and process their passengers’ PNR data for their own commercial purposes. This Directive should not impose any obligation on air carriers to collect or retain any additional data from passengers or any obligation on passengers to provide any data in addition to that already being provided to air carriers.  
(9)      Some air carriers retain as part of the PNR data the API data they collect, while others do not. The use of PNR data together with API data has added value in assisting Member States in verifying the identity of an individual, thus reinforcing the law enforcement value of that result and minimising the risk of carrying out checks and investigations on innocent people. It is therefore important to ensure that where air carriers collect API data, they transfer it irrespective of whether they retain API data by different technical means as for other PNR data.  
(10)      To prevent, detect, investigate and prosecute terrorist offences and serious crime, it is essential that all Member States introduce provisions laying down obligations on air carriers operating extra-EU flights to transfer PNR data they collect, including API data. Member States should also have the possibility to extend this obligation to air carriers operating intra-EU flights. Those provisions should be without prejudice to [the API Directive].  
(11)      The processing of personal data should be proportionate to the specific security goals pursued by this Directive.  
(12)      The definition of terrorist offences applied in this Directive should be the same as in Council Framework Decision 2002/475/JHA [of 13 June 2002 on combating terrorism (OJ 2002 L 164, p. 3)]. The definition of serious crime should encompass the categories of offence listed in Annex II to this Directive.  
…  
(15)      A list of the PNR data to be obtained by a [passenger information unit (PIU)] should be drawn up with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the Union as well as protecting the fundamental rights, in particular privacy and the protection of personal data. To that end, high standards should be applied in accordance with [the Charter], the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention No 108”), and the European Convention for the Protection of Human Rights and Fundamental Freedom[, signed at Rome on 4 November 1950] (the “ECHR”). Such a list should not be based on a person’s race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation. The PNR data should only contain details of passengers’ reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security.  
…  
(19)      Each Member State should be responsible for assessing the potential threats related to terrorist offences and serious crime.  
(20)      Taking fully into consideration the right to the protection of personal data and the right to non-discrimination, no decision that produces an adverse legal effect on a person or significantly affects that person should be taken only by reason of the automated processing of PNR data. Moreover, in respect of Articles 8 and 21 of the Charter, no such decision should discriminate on any grounds such as a person’s sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. The [European] Commission should also take those principles into account when reviewing the application of this Directive.  
…  
(22)      Taking fully into consideration the principles outlined in recent relevant case-law of the Court of Justice of the European Union, the application of this Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality. It should also genuinely meet the objectives of necessity and proportionality in order to achieve the general interests recognised by the [European] Union and the need to protect the rights and freedoms of others in the fight against terrorist offences and serious crime. The application of this Directive should be duly justified and the necessary safeguards put in place to ensure the lawfulness of any storage, analysis, transfer or use of PNR data.  
…  
(25)      The period during which PNR data are to be retained should be as long as is necessary for and proportionate to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Because of the nature of the data and their uses, it is necessary that the PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations. To avoid disproportionate use, after the initial retention period the PNR data should be depersonalised through masking out of data elements. To ensure the highest level of data protection, access to the full PNR data, which enable direct identification of the data subject, should be granted only under very strict and limited conditions after that initial period.  
…  
(27)      The processing of PNR data in each Member State by the PIU and by competent authorities should be subject to a standard of protection of personal data under national law in line with Framework Decision [2008/977] and the specific data protection requirements laid down in this Directive. References to Framework Decision [2008/977] should be understood as references to legislation currently in force as well as to legislation that will replace it.  
(28)      Taking into consideration the right to the protection of personal data, the rights of data subjects concerning the processing of their PNR data, such as the rights of access, rectification, erasure and restriction and the rights to compensation and judicial redress, should be in line both with Framework Decision [2008/977] and with the high level of protection provided by the Charter and the ECHR.  
…  
(33)      This Directive does not affect the possibility for Member States to provide, under their national law, for a system of collecting and processing PNR data from non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services – including the booking of flights – for which they collect and process PNR data, or from transportation providers other than those specified in this Directive, provided that such national law complies with [EU] law.  
…  
(36)      This Directive respects the fundamental rights and the principles of the Charter, in particular the right to the protection of personal data, the right to privacy and the right to non-discrimination as protected by Articles 8, 7 and 21 thereof; it should therefore be implemented accordingly. This Directive is compatible with data protection principles and its provisions are in line with Framework Decision [2008/977]. Furthermore, to comply with the proportionality principle, on specific issues this Directive provides for stricter rules on data protection than Framework Decision [2008/977].  
(37)      The scope of this Directive is as limited as possible since: it provides for the retention of PNR data in the PIUs for a period of time not exceeding five years, after which the data should be deleted; it provides for the data to be depersonalised through masking out of data elements after an initial period of six months; and it prohibits the collection and use of sensitive data. To ensure efficiency and a high level of data protection, Member States are required to ensure that an independent national supervisory authority and, in particular, a data protection officer are responsible for advising and monitoring the way PNR data are processed. All processing of PNR data should be logged or documented for the purposes of verifying its legality, self-monitoring and ensuring proper data integrity and secure processing. Member States should also ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.’  
23      Article 1 of the PNR Directive, entitled ‘Subject matter and scope’, is worded as follows:  
‘1.      This Directive provides for:  
(a)      the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights,  
(b)      the processing of the data referred to in point (a), including its collection, use and retention by Member States and its exchange between Member States.  
2.      PNR data collected in accordance with this Directive may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in points (a), (b) and (c) of Article 6(2).’  
24      In accordance with Article 2 of that directive, entitled ‘Application of this Directive to intra-EU flights’:  
‘1.      If a Member State decides to apply this Directive to intra-EU flights, it shall notify the Commission in writing. A Member State may give or revoke such a notification at any time. The Commission shall publish that notification and any revocation of it in the   
Official Journal of the European Union  
.  
2.      Where a notification referred to in paragraph 1 is given, all the provisions of this Directive shall apply to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if they were PNR data from extra-EU flights.  
3.      A Member State may decide to apply this Directive only to selected intra-EU flights. In making such a decision, the Member State shall select the flights it considers necessary in order to pursue the objectives of this Directive. The Member State may decide to change the selection of intra-EU flights at any time.’  
25      Under Article 3 of that directive, entitled ‘Definitions’:  
‘For the purposes of this Directive the following definitions apply:  
(1)      “air carrier” means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage of passengers by air;  
(2)      “extra-EU flight” means any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the territory of a Member State or flying from the territory of a Member State and planned to land in a third country, including in both cases flights with any stop-overs in the territory of Member States or third countries;  
(3)      “intra-EU flight” means any scheduled or non-scheduled flight by an air carrier flying from the territory of a Member State and planned to land on the territory of one or more of the other Member States, without any stop-overs in the territory of a third country;   
(4)      “passenger” means any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, such consent being manifested by that person’s registration in the passengers list;  
(5)      “passenger name record” or “PNR” means a record of each passenger’s travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities;  
(6)      “reservation system” means the air carrier’s internal system, in which PNR data are collected for the handling of reservations;  
(7)      “push method” means the method whereby air carriers transfer PNR data listed in Annex I into the database of the authority requesting them;  
(8)      “terrorist offences” means the offences under national law referred to in Articles 1 to 4 of Framework Decision [2002/475];  
(9)      “serious crime” means the offences listed in Annex II that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State;  
(10)      “to depersonalise through masking out of data elements” means to render those data elements which could serve to identify directly the data subject invisible to a user.’  
26      Article 4 of the PNR Directive, entitled ‘Passenger information unit’, provides in paragraphs 1 to 3:  
‘1.      Each Member State shall establish or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime or a branch of such an authority, to act as its passenger information unit (“PIU”).  
2.      The PIU shall be responsible for:  
(a)      collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities referred to in Article 7;  
(b)      exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with Europol in accordance with Articles 9 and 10.  
3.      Staff members of a PIU may be seconded from competent authorities. Member States shall provide the PIUs with adequate resources for them to fulfil their tasks.’  
27      Article 5 of that directive, entitled ‘Data protection officer in the PIU’ is worded as follows:  
‘1.      The PIU shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards.  
2.      Member States shall provide data protection officers with the means to perform their duties and tasks in accordance with this Article effectively and independently.  
3.      Member States shall ensure that a data subject has the right to contact the data protection officer, as a single point of contact, on all issues relating to the processing of that data subject’s PNR data.’  
28      Article 6 of that directive, entitled ‘Processing of PNR data’, provides that:  
‘1.      The PNR data transferred by the air carriers shall be collected by the PIU of the relevant Member State as provided for in Article 8. Where the PNR data transferred by air carriers include data other than those listed in Annex I, the PIU shall delete such data immediately and permanently upon receipt.  
2.      The PIU shall process PNR data only for the following purposes:  
(a)      carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities referred to in Article 7, and, where relevant, by Europol in accordance with Article 10, in view of the fact that such persons may be involved in a terrorist offence or serious crime;  
(b)      responding, on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, and to provide the competent authorities or, where appropriate, Europol with the results of such processing; and  
(c)      analysing PNR data for the purpose of updating or creating new criteria to be used in the assessments carried out under point (b) of paragraph 3 in order to identify any persons who may be involved in a terrorist offence or serious crime.   
3.      When carrying out the assessment referred to in point (a) of paragraph 2, the PIU may:  
(a)      compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases; or  
(b)      process PNR data against pre-determined criteria.  
4.      Any assessment of passengers prior to their scheduled arrival in or departure from the Member State carried out under point (b) of paragraph 3 against pre-determined criteria shall be carried out in a non-discriminatory manner. Those pre-determined criteria must be targeted, proportionate and specific. Member States shall ensure that those criteria are set and regularly reviewed by the PIU in cooperation with the competent authorities referred to in Article 7. The criteria shall in no circumstances be based on a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.  
5.      Member States shall ensure that any positive match resulting from the automated processing of PNR data conducted under point (a) of paragraph 2 is individually reviewed by non-automated means to verify whether the competent authority referred to in Article 7 needs to take action under national law.  
6.      The PIU of a Member State shall transmit the PNR data of persons identified in accordance with point (a) of paragraph 2 or the result of processing those data for further examination to the competent authorities referred to in Article 7 of the same Member State. Such transfers shall only be made on a case-by-case basis and, in the event of automated processing of PNR data, after individual review by non-automated means.  
7.      Member States shall ensure that the data protection officer has access to all data processed by the PIU. If the data protection officer considers that processing of any data has not been lawful, the data protection officer may refer the matter to the national supervisory authority.  
…   
9.      The consequences of the assessments of passengers referred to in point (a) of paragraph 2 of this Article shall not jeopardise the right of entry of persons enjoying the [EU] right of free movement into the territory of the Member State concerned as laid down in Directive 2004/38/EC of the European Parliament and of the Council [of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ 2004 L 158, p. 77)]. In addition, where assessments are carried out in relation to intra-EU flights between Member States to which Regulation (EC) No 562/2006 of the European Parliament and of the Council [of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ 2006 L 105, p. 1)] applies, the consequences of such assessments shall comply with that Regulation.’  
29      Under Article 7 of the PNR Directive, entitled ‘Competent authorities’:  
‘1.      Each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU in order to examine that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.  
2.      The authorities referred to in paragraph 1 shall be authorities competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime.  
…  
4.      The PNR data and the result of processing those data received by the PIU may be further processed by the competent authorities of the Member States only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.  
5.      Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing.  
6.      The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.’  
30      Article 8 of that directive, entitled ‘Obligations on air carriers regarding transfers of data’, provides in its paragraphs 1 to 3:  
‘1.      Member States shall adopt the necessary measures to ensure that air carriers transfer, by the “push method”, the PNR data listed in Annex I, to the extent that they have already collected such data in the normal course of their business, to the database of the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart. Where the flight is code-shared between one or more air carriers, the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight. Where an extra-EU flight has one or more stop-overs at airports of the Member States, air carriers shall transfer the PNR data of all passengers to the PIUs of all the Member States concerned. This also applies where an intra-EU flight has one or more stop-overs at the airports of different Member States, but only in relation to Member States which are collecting PNR data from intra-EU flights.  
2.      In the event that the air carriers have collected any [API] data listed under item 18 of Annex I but do not retain those data by the same technical means as for other PNR data, Member States shall adopt the necessary measures to ensure that air carriers also transfer, by the “push method”, those data to the PIU of the Member States referred to in paragraph 1. In the event of such a transfer, all the provisions of this Directive shall apply in relation to those API data.  
3.      Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with the examination procedure referred to in Article 17(2) or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:  
(a)      24 to 48 hours before the scheduled flight departure time; and  
(b)      immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.’  
31      Article 12 of that directive, entitled ‘Period of data retention and depersonalisation’, provides:  
‘1.      Member States shall ensure that the PNR data provided by the air carriers to the PIU are retained in a database at the PIU for a period of five years after their transfer to the PIU of the Member State on whose territory the flight is landing or departing.  
2.      Upon expiry of a period of six months after the transfer of the PNR data referred to in paragraph 1, all PNR data shall be depersonalised through masking out of the following data elements which could serve to identify directly the passenger to whom the PNR data relate:  
(a)      name(s), including the names of other passengers on the PNR and number of travellers on the PNR travelling together;  
(b)      address and contact information;  
(c)      all forms of payment information, including billing address, to the extent that it contains any information which could serve to identify directly the passenger to whom the PNR relate or any other persons;  
(d)      frequent flyer information;  
(e)      general remarks to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate; and  
(f)      any API data that have been collected.  
3.      Upon expiry of the period of six months referred to in paragraph 2, disclosure of the full PNR data shall be permitted only where it is:  
(a)      reasonably believed that it is necessary for the purposes referred to in point (b) of Article 6(2) and  
(b)      approved by:  
(i)      a judicial authority; or  
(ii)      another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an   
ex post  
 review by that data protection officer.  
4.      Member States shall ensure that the PNR data are deleted permanently upon expiry of the period referred to in paragraph 1. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific cases for the purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, in which case the retention of such data by the competent authority shall be regulated by national law.  
5.      The result of the processing referred to in point (a) of Article 6(2) shall be kept by the PIU only as long as necessary to inform the competent authorities and, in accordance with Article 9(1), to inform the PIUs of other Member States of a positive match. Where the result of automated processing has, further to individual review by non-automated means as referred to in Article 6(5), proven to be negative, it may, however, be stored so as to avoid future “false” positive matches for as long as the underlying data are not deleted under paragraph 4 of this Article.’  
32      Article 13 of the PNR Directive, entitled ‘Protection of personal data’, provides in paragraphs 1 to 5:  
‘1.      Each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress as laid down in [EU] and national law and in implementation of Articles 17, 18, 19 and 20 of Framework Decision [2008/977]. Those Articles shall therefore apply.  
2.      Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of Framework Decision [2008/977] regarding confidentiality of processing and data security shall also apply to all processing of personal data pursuant to this Directive.  
3.      This Directive is without prejudice to the applicability of Directive [95/46] to the processing of personal data by air carriers, in particular their obligations to take appropriate technical and organisational measures to protect the security and confidentiality of personal data.  
4.      Member States shall prohibit the processing of PNR data revealing a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information are received by the PIU, they shall be deleted immediately.  
5.      Member States shall ensure that the PIUs maintain documentation relating to all processing systems and procedures under their responsibility. That documentation shall contain at least:  
(a)      the name and contact details of the organisation and personnel in the PIU entrusted with the processing of the PNR data and the different levels of access authorisation;  
(b)      the requests made by competent authorities and PIUs of other Member States;  
(c)      all requests for and transfers of PNR data to a third country.  
The PIU shall make all documentation available, upon request, to the national supervisory authority.’  
33      According to Article 15 of that directive, entitled ‘National supervisory authority’:  
‘1.      Each Member State shall provide that the national supervisory authority referred to in Article 25 of Framework Decision [2008/977] is responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. Article 25 of Framework Decision [2008/977] shall apply.  
2.      Those national supervisory authorities shall conduct activities under paragraph 1 with a view to protecting fundamental rights in relation to the processing of personal data.  
3.      Each national supervisory authority shall:  
(a)      deal with complaints lodged by any data subject, investigate the matter and inform the data subjects of the progress and the outcome of their complaints within a reasonable time period;  
(b)      verify the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint referred to in point (a).  
4.      Each national supervisory authority shall, upon request, advise any data subject on the exercise of the rights laid down in provisions adopted pursuant to this Directive.’  
34      Article 19 of the directive, entitled ‘Review’, provides:  
‘1.      On the basis of information provided by the Member States, including the statistical information referred to in Article 20(2), the Commission shall by 25 May 2020 conduct a review of all the elements of this Directive and submit and present a report to the European Parliament and to the Council [of the European Union].  
2.      In conducting its review, the Commission shall pay special attention to:  
(a)      compliance with the applicable standards of protection of personal data,  
(b)      the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in this Directive,  
(c)      the length of the data retention period,  
(d)      the effectiveness of exchange of information between the Member States, and  
(e)      the quality of the assessments including with regard to the statistical information gathered pursuant to Article 20.  
3.      The report referred to in paragraph 1 shall also include a review of the necessity, proportionality, and effectiveness of including within the scope of this Directive the mandatory collection and transfer of PNR data relating to all or selected intra-EU flights. The Commission shall take into account the experience gained by Member States, especially those Member States that apply this Directive to intra-EU flights in accordance with Article 2. The report shall also consider the necessity of including non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services, including the booking of flights, within the scope of this Directive.  
4.      If appropriate, in light of the review conducted pursuant to this Article, the Commission shall make a legislative proposal to the European Parliament and to the Council with a view to amending this Directive.’  
35      Article 21 of that directive, entitled ‘Relationship to other instruments’, provides, in paragraph 2:  
‘This Directive is without prejudice to the applicability of Directive [95/46] to the processing of personal data by air carriers.’  
36      Annex I to the PNR Directive, entitled ‘Passenger name record data as far as collected by air carriers’, provides:  
‘1.      PNR record locator  
2.      Date of reservation/issue of ticket  
3.      Date(s) of intended travel  
4.      Name(s)  
5.      Address and contact information (telephone number, email address)  
6.      All forms of payment information, including billing address  
7.      Complete travel itinerary for specific PNR  
8.      Frequent flyer information  
9.      Travel agency/travel agent  
10.      Travel status of passenger, including confirmations, check-in status, no-show or go-show information  
11.      Split/divided PNR information  
12.      General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)  
13.      Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields  
14.      Seat number and other seat information  
15.      Code share information  
16.      All baggage information  
17.      Number and other names of travellers on the PNR  
18.      Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)  
19.      All historical changes to the PNR listed in numbers 1 to 18.’  
37      Annex II to that directive, entitled ‘List of offences referred to in point (9) of Article 3’, is worded as follows:  
‘1.      participation in a criminal organisation,  
2.      trafficking in human beings,  
3.      sexual exploitation of children and child pornography,  
4.      illicit trafficking in narcotic drugs and psychotropic substances,  
5.      illicit trafficking in weapons, munitions and explosives,  
6.      corruption,  
7.      fraud, including that against the financial interests of the Union,  
8.      laundering of the proceeds of crime and counterfeiting of currency, including the euro,  
9.      computer-related crime/cybercrime,  
10.      environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,  
11.      facilitation of unauthorised entry and residence,  
12.      murder, grievous bodily injury,  
13.      illicit trade in human organs and tissue,  
14.      kidnapping, illegal restraint and hostage-taking,  
15.      organised and armed robbery,  
16.      illicit trafficking in cultural goods, including antiques and works of art,  
17.      counterfeiting and piracy of products,  
18.      forgery of administrative documents and trafficking therein,  
19.      illicit trafficking in hormonal substances and other growth promoters,  
20.      illicit trafficking in nuclear or radioactive materials,  
21.      rape,  
22.      crimes within the jurisdiction of the International Criminal Court,  
23.      unlawful seizure of aircraft/ships,  
24.      sabotage,  
25.      trafficking in stolen vehicles,  
26.      industrial espionage.’  
7.        
Framework Decision 2002/475  
38      Article 1 of Framework Decision 2002/475 defined the concept of ‘terrorist offence’ by listing intentional acts referred to in points (a) to (i) of that article, committed with the aim of ‘seriously intimidating a population’, ‘unduly compelling a Government or international organisation to perform or abstain from performing any act’, or ‘seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation’. Articles 2 and 3 of that framework decision defined the concepts of ‘offences relating to a terrorist group’ and of ‘offences linked to terrorist activities’, respectively. Article 4 of the said framework decision governed the charges of inciting and aiding or abetting those offences as well as that of attempting to commit them.  
39      Framework Decision 2002/475 was repealed by Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Framework Decision 2002/475 and amending Council Decision 2005/671/JHA (OJ 2017 L 88, p. 6), Articles 3 to 14 of which include similar definitions.  
B.        
Belgian law  
1.        
The Constitution  
40      Article 22 of the Constitution provides as follows:  
‘Everyone is entitled to respect for private and family life except in the cases and under the circumstances laid down by law.  
The laws, decrees and rules referred to in Article 134 guarantee the protection of this right.’  
2.        
The Law of 25 December 2016  
41      Article 2 of the loi du 25 décembre 2016, relative au traitement des données des passagers (Law of 25 December 2016 on the processing of passenger data,   
Moniteur belge  
 of 25 January 2017, p. 12905; ‘the Law of 25 December 2016’) is worded as follows:  
‘The present law and the royal decrees which shall be adopted in implementation of the present law transpose [the API Directive] and [the PNR Directive]. The present law and the royal decree concerning the maritime sector partially transpose Directive [2010/65].’  
42      Article 3 of that law provides:  
‘1.      This law lays down the obligations of carriers and tour operators regarding the transfer of data relating to passengers travelling to or from or transiting through Belgian territory.  
2.      The King shall prescribe, by decree deliberated in the Council of Ministers, in respect of each sector of the transport industry and in respect of tour operators, the passenger data to be transferred and how they are to be transferred, after an opinion has been given by the Commission de la protection de la vie privée [(Commission for the protection of privacy)].’  
43      Under Article 4 of that law:  
‘For the purposes of this law and its implementing decrees, the following definitions shall apply:  
…  
(8)      “the competent services”: the services under Article 14(1)(2);  
(9)      “PNR”: a record of each passenger’s travel requirements which contains the information referred to in Article 9, which is necessary to enable reservations to be processed and controlled by the booking and participating carriers and tour operators for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities;  
(10)      “passenger”: any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried by the carrier with its consent, such consent being manifested by that person’s registration in the passengers list;  
…’  
44      Article 8 of the Law of 25 December 2016 states:  
‘1.      Passenger data shall be processed for the purposes of:  
(1)      detection and prosecution (including the execution of penalties or measures depriving the person concerned of his or her liberty) of the offences referred to Article 90  
ter  
(2), …(7), …(8), …(11), …(14), …(17), (18), (19) and Article 90  
ter  
(3) of the Code d’instruction criminelle [(Criminal Procedure Code)];  
(2)      detection and prosecution (including the execution of penalties or measures depriving the person of his or her liberty) of the offences referred to in Article 196, in so far as concerns the offences of forgery of authentic and public documents, Article 198, 199, 199  
bis  
, 207, 213, 375 and 505 of the Code pénal [(Criminal Code)];  
…  
(4)      monitoring the activities referred to in Article 7(1) and (3/l) and Article 11(1)(1) to (3) and (5) of the loi du 30 novembre 1998 organique des services de renseignement et de sécurité [(Organic law of 30 November 1998 on the intelligence and security services)];  
(5)      detection and prosecution of the offences referred to in Article 220(2) of the loi générale sur les douanes et accises du 18 juillet 1977 [(General customs and excise law of 18 July 1977)] and the third paragraph of Article 45 of the loi du 22 décembre 2009 relative au régime général d’accise [(Law of 22 December 2009 on the general excise regime)] …  
2.      Subject to the conditions in Chapter 11, passenger data shall also be processed with a view to improving external border controls on individuals, and with a view to combating illegal immigration.’  
45      Article 14(1) of that law states:  
‘The PIU shall be made up of:  
…  
(2)      members seconded from the following competent services:  
(a)      the police services covered by the loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux [(Law of 7 December 1998 organising an integrated police service, with a two-tier structure)];  
(b)      the Sûreté de l’État [(State security services)] covered by the [Organic law of 30 November 1998 on the intelligence and security services];  
(c)      the Service général de Renseignement et de Sécurité [(General intelligence and security services)] covered by the [Organic law of 30 November 1998 on the intelligence and security services];  
…’  
46      Article 24 of the said law, in Section 1 thereof, entitled ‘Processing of passenger data in connection with the advance assessment of passengers’, of Chapter 10 of that law, on data processing, is worded as follows:  
‘1.      Passenger data shall be processed with a view to carrying out an assessment of passengers prior to their scheduled arrival in, departure from, or transit through Belgian territory, in order to identify persons who require further examination.  
2.      For the purposes referred to in Article 8(1)(1), (4) and (5), or relating to the threats referred to in Article 8(1)(a), (b), (c), (d), (f) and (g) and Article 11(2) of the [Organic law of 30 November 1998 on the intelligence and security services], the advance assessment of passengers shall be based on a positive match resulting from comparing passenger data against:  
(1)      the databases managed by the competent services or which are directly available or accessible to those services in the course of their functions or against the lists of individuals drawn up by the competent services in the course of their functions.  
(2)      the assessment criteria pre-determined by the PIU, as referred to in Article 25.  
3.      For the purposes referred to in Article 8(1)(3), the advance assessment of passengers shall be based on a positive match resulting from comparing passenger data against the databases referred to in Article 8(2)(1).  
4.      Positive matches shall be validated by the PIU within 24 hours of receipt of the automated notification of the positive match.  
5.      From the moment of that validation, the competent service which originally identified the positive match shall take further action without delay.’  
47      Chapter 11 of the Law of 25 December 2016, entitled ‘Processing of passenger data with a view to improving border controls and combating illegal immigration’, comprises Articles 28 to 31 thereof.  
48      Article 28 of that law provides:  
‘1.      This Chapter applies to the processing of passenger data by the police services responsible for carrying out border checks and by the Office des étrangers [(Immigration Office)], carried out with a view to improving the checks on persons at external borders and with a view to combating illegal immigration.  
2.      It applies without prejudice to the obligations incumbent on the police services responsible for carrying out border checks and on the [Immigration Office] to transfer personal data or information in accordance with legal or statutory provisions.’  
49      Under Article 29 of that law:  
‘1.      For the purposes of Article 28(1) passenger data are transferred to the police services responsible for carrying out border checks and to the [Immigration Office] to enable them to perform their statutory duties, within the limits provided for in this article.  
2.      Only the passenger data referred to in Article 9(1)(18) concerning the following passenger categories shall be transferred:  
(1)      passengers who intend to enter or have entered Belgian territory at an external border;  
(2)      passengers who intend to leave or have left Belgian territory at an external border;  
(3)      passengers who intend to pass through, are located in, or have passed through an international transit area situated on Belgian territory.  
3.      The passenger data referred to in paragraph (2) shall be transferred to the police services responsible for carrying out checks at Belgium’s external border immediately after they have been entered in the passenger database. The said services shall save those data in a temporary file and delete them within 24 hours of the transfer.  
4.      When it needs them to perform its statutory duties, the passenger data referred to in paragraph (2) shall be transferred to the [Immigration Office] immediately after they have been entered in the passenger database. The Office shall save those data in a temporary file and delete them within 24 hours of the transfer.  
After that period has passed, if the [Immigration Office] requires access to the passenger data referred to in paragraph (2) for the purposes of performing its statutory duties, it shall send a duly reasoned request to the PIU.  
…’  
50      The Law of 25 December 2016 became applicable to airlines, carriers operating international passenger service (HST carriers) and travel intermediaries in a contract with those carriers (HST ticket distributors), and bus carriers, respectively, by the arrêté royal du 1 juillet 2017 relatif à l’exécution de la loi du 25 décembre 2016, reprenant les obligations pour les compagnies aériennes (Royal Decree of 18 July 2017 implementing the Law of 25 December 2016 on the obligations incumbent on airlines,   
Moniteur belge  
 of 28 July 2017, p. 75934), by the arrêté royal du 3 février 2019 relatif à l’exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs HST et distributeurs de tickets HST (Royal Decree of 3 February 2019 implementing the Law of 25 December 2016 on the obligations incumbent on HST carriers and HST ticket distributors,   
Moniteur belge  
 of 12 Feburary 2019, p. 13018) and by the arrêté royal du 3 février 2019 relatif à l’exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs par bus (Royal Decree of 3 February 2019 implementing the Law of 25 December 2016 on the obligations incumbent on bus carriers,   
Moniteur belge  
 of 12 February 2019, p. 13023).  
II.      
The dispute in the main proceedings and the questions referred for a preliminary ruling  
51      By application of 24 July 2017, the Ligue des droits humains brought an action before the Cour constitutionnelle (Constitutional Court, Belgium) seeking annulment in full or in part of the Law of 25 December 2016.  
52      The referring court states that that law transposes, into domestic law, the PNR Directive and the API Directive as well as, in part, Directive 2010/65. According to the referring court, it follows from the   
travaux préparatoires  
 that that law seeks to ‘create a legal framework requiring international passenger transport carriers in various sectors (air, rail, international road and sea), as well as tour operators, to transfer data on their passengers to a database managed by the [Service public fédéral intérieur (Home Affairs Federal Public Service, Belgium)]’. The national legislature also stated that the intended purposes of the Law of 25 December 2016 fall into three categories, namely (i) the prevention, detection, investigation and prosecution of criminal offences or the enforcement of criminal penalties; (ii) the tasks of the intelligence and security services; and (iii) improving external border controls and combating illegal immigration.  
53      In support of its action, the Ligue des droits humains raises two pleas, the first, alleging breach of Article 22 of the Constitution, read in conjunction with Article 23 of the GDPR, Articles 7, 8 as well as Article 52(1) of the Charter as well as Article 8 ECHR, and the second, alleging, in the alternative, breach of Article 22 of the Charter, read in conjunction with Article 3(2) TEU and Article 45 of the Charter.  
54      By its first plea, the Ligue des droits humains submits, in essence, that that law entails an interference with the rights to respect for private life and the protection of personal data, which does not comply with Article 52(1) of the Charter and, inter alia, the principle of proportionality. The scope of that law and the definition of the data collected, which may reveal sensitive information, are too broad. Similarly, the concept of ‘passenger’, within the meaning of that same law, leads to systematic, non-targeted automated processing of the data of all passengers. Moreover, the nature and detailed rules of the ‘pre-screening’ method and the databases against which those data are compared, once transmitted, are not defined in a sufficiently clear manner. Furthermore, the Law of 25 December 2016 pursues objectives other than those of the PNR Directive. Finally, the five-year period laid down by that law for the retention of those data is disproportionate.  
55      By its second plea, concerning Article 3(1), Article 8(2) and Articles 28 to 31 of the Law of 25 December 2016, the Ligue des droits humains submits that, by extending the system provided for by the PNR Directive to intra-EU transport operations, those provisions have the effect of indirectly restoring internal border control, in breach of the free movement of persons. Once a person is on Belgian territory, whether on arrival, departure or during a stop-over, their data are automatically collected.  
56      The Council of Ministers disputes those arguments. It considers, in particular, that the first plea is inadmissible in so far as it concerns the GDPR, which is not applicable to the Law of 25 December 2016. Furthermore, the processing of data provided for by that law, in accordance with the PNR Directive, is an essential tool for, inter alia, the fight against terrorism and serious crime, and the measures stemming from that law are necessary to achieve the aims pursued and are proportionate.  
57      As regards the first plea, the referring court asks, first of all, whether the protection provided for by the GDPR applies to the processing of data established by the Law of 25 December 2016, which is intended to implement, primarily, the PNR Directive. Next, that court notes, with reference to the case-law stemming from Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017 (EU:C:2017:592), that the definition of PNR data in Article 3(5) of and Annex I to that directive may, first, not be sufficiently clear and precise, on account of the non-exhaustive nature of the description of some of those data contained in those provisions and, secondly, lead indirectly to the disclosure of sensitive data. Furthermore, the definition of the concept of ‘passenger’ in Article 3(4) of that directive may result in the collection, transfer, processing and retention of PNR data constituting generalised and indiscriminate obligations, applying to every person carried or to be carried who appears on the passengers list, regardless of whether there are serious grounds for believing that that person has committed or is about to commit an offence or has been found guilty of an offence.  
58      The referring court also observes that PNR data, in accordance with the provisions of the PNR Directive, are systematically subject to advance assessment involving cross-checks with databases or pre-determined criteria with a view to finding matches. The Consultative Committee of Convention No 108 of the Council of Europe indicated in its Opinion of 19 August 2016 on the Data protection implications of the processing of Passenger Name Records (T-PD(2016)18rev) that the processing of personal data concerns all passengers and not only the targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order, and that PNR data may not only be compared (‘data matching’) to databases but also be processed by ‘data mining’ according to selectors or predictive algorithms, with the aim of identifying anyone who may be involved or might engage in criminal activities, as this assessment of passengers by data mining may raise the question of predictability, in particular when operated on the basis of predictive algorithms using dynamic criteria that may constantly evolve in light of self-learning capacities. In that context, the referring court considers that, although the pre-determined criteria for identifying high-risk profiles must be specific, reliable and non-discriminatory, in accordance with Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017 (EU:C:2017:592), it seems to be impossible technically to define those criteria further.  
59      As regards the five-year retention period and access to the data provided for in Article 12 of the PNR Directive, the referring court notes that the Commission for the protection of privacy (Belgium), in its avis d’initiative no 01/2010 du 13 janvier 2010 relatif au projet de loi portant assentiment à l’accord PNR UE-États-Unis d’Amérique (own-initiative Opinion No 01/2010 of 13 January 2010 on the Draft law ratifying the PNR Agreement between the European Union and the United States of America), considered that when data is retained for a long period and is stored   
en masse  
, the risk of the data subjects being profiled rises, as does the potential for improper use of the data for purposes other than those originally intended. It is also apparent from the Opinion of 19 August 2016 of the Consultative Committee of Convention No 108 of the Council of Europe that masked out data still enables individuals to be identified and continue as such to constitute personal data, and that their retention should be limited in time in order to avoid permanent and general surveillance.  
60      In those circumstances, having regard to the case-law resulting in particular from Opinion 1/15   
(EU-Canada PNR Agreement  
)  
) of 26 July 2017 (EU:C:2017:592), the referring court asks whether the system for the collection, transfer, processing and retention of PNR data established by the PNR Directive may be regarded as coming within the limits of what is strictly necessary. That court considers that it is also appropriate to ascertain whether that directive precludes national legislation authorising the processing of PNR data for a purpose other than that provided for by that directive and whether disclosure of the full data after they have been depersonalised, pursuant to Article 12 of that directive, may be approved by a national authority such as the PIU created by the Law of 25 December 2016.  
61      As regards the second plea, the referring court states that Article 3(1) of that law lays down the obligations of carriers and tour operators regarding the transfer of data relating to passengers ‘travelling to or from or transiting through Belgian territory’. That court adds, with regard to the scope of that law, that the national legislature decided to ‘inclu[de] intra-EU travel in the data collection’ in order to obtain ‘a fuller picture of passenger movements representing a potential threat to intra-Community and national security’, as envisaged by Article 2 of the PNR Directive, read in conjunction with recital 10 thereof, for flights within the European Union. The referring court also states that the Commission for the protection of privacy, in its Opinion No 55/2015 of 16 December 2015 on the draft bill which became the Law of 25 December 2016, had raised the issue of whether the Belgian PNR system might conflict with the principle of the free movement of persons, in so far as that system includes transport operations carried out within the European Union.  
62      It is in those circumstances that the Cour constitutionnelle (Constitutional Court) decided to stay proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 23 of [the GDPR], read in conjunction with Article 2(2)(d) of that regulation, to be interpreted as applying to national legislation such as the [Law of 25 December 2016], which transposes [the PNR Directive] as well as [the API Directive] and Directive [2010/65]?  
(2)      Is Annex I to [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that the data it refers to are very wide in scope – particularly the data referred to in paragraph 18 of Annex I to [that directive], which go beyond the data referred to in Article 3(2) of [the API Directive] – and also given that, taken together, they may reveal sensitive information, and thus go beyond what is “strictly necessary”?  
(3)      Are paragraphs 12 and 18 of Annex I to [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that, having regard to the word “including”, the data referred to in those paragraphs is given by way of example and not exhaustively, such that the requirement for precision and clarity in rules which interfere with the right to respect for private life and the right to protection of personal data is not satisfied?  
(4)      Are Article 3(4) of [the PNR Directive] and Annex I to that directive compatible with Articles 7, 8 and 52(1) of [the Charter], given that the system of generalised collection, transfer and processing of passenger data established by those provisions relates to any person using the mode of transport concerned, regardless of whether there is any objective ground for considering that that person may present a risk to public security?  
(5)      Is Article 6 of [the PNR Directive], read in conjunction with Articles 7, 8 and 52(1) of [the Charter], to be interpreted as precluding national legislation such as the contested law, which includes, among the purposes for which PNR data is processed, [monitoring] activities within the remit of the intelligence and security services, thus treating that purpose as an integral part of the prevention, detection, investigation and prosecution of terrorist offences and serious crime?  
(6)      Is Article 6 of [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that the advance assessment for which it provides, which is made by comparing passenger data against databases and pre-determined criteria, applies to such data in a systematic and generalised manner, regardless of whether there is any objective ground for considering that the passengers concerned may present a risk to public security?  
(7)      Can the expression “another national authority competent under national law” in Article 12(3) of [the PNR Directive] be interpreted as including the PIU created by the Law of 25 December 2016, which would then have power to authorise access to PNR data after six months had passed, for the purposes of ad hoc searches?  
(8)      Is Article 12 of [the PNR Directive], read in conjunction with Articles 7, 8 and 52(1) of [the Charter], to be interpreted as precluding national legislation such as the contested law which provides for a general data retention period of five years, without making any distinction in terms of whether the advance assessment indicated that the passengers might present a risk to public security?  
(9)      (a)      Is [the API Directive] compatible with Article 3(2) [TEU] and Article 45 of [the Charter], given that the obligations for which it provides apply to flights within the European Union?  
(b)      Is [the API Directive], read in conjunction with Article 3(2) [TEU] and Article 45 of [the Charter], to be interpreted as precluding national legislation such as the contested law which, for the purposes of combating illegal immigration and improving border controls, authorises a system of collection and processing of data relating to passengers “travelling to, from or transiting through Belgian territory”, which may indirectly involve a re-establishment of internal border controls?  
(10)      If, on the basis of the answers to the preceding questions, the Cour constitutionnelle (Constitutional Court) concludes that the contested law, which transposes, inter alia, [the PNR Directive], fails to fulfil one or more of the obligations arising under the provisions referred to in those questions, would it be open to it to maintain the effects of the [Law of 25 December 2016], on a temporary basis, in order to avoid legal uncertainty and enable the data hitherto collected and retained to continue to be used for the purposes envisaged by the law?’  
III.   
Consideration of the questions referred  
A.        
Question 1  
63      By its Question 1, the referring court asks, in essence, whether Article 2(2)(d) and Article 23 of the GDPR must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of the PNR Directive, those of the API Directive and also those of Directive 2010/65, in particular, the transfer, the retention and the processing of PNR data.  
64      As is apparent from Article 2(1) of the GDPR, that regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of such data which form part of a filing system or are intended to form part of a filing system. The concept of ‘processing’ is defined in broad terms in Article 4(2) of that regulation as including, inter alia, collection, recording, storage, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or erasure of such data or sets of data.  
65      The Belgian Government submits however that the transfer of PNR data by economic operators to the PIU, for the purposes of the prevention and detection of criminal offences, as provided for in Article 1(1)(a) and (2) and Article 8 of the PNR Directive, which constitutes ‘processing’ of personal data within the meaning of Article 4(2) of the GDPR, as well as the advance collection thereof, fall outside the scope of Article 2(2)(d) of the said regulation, on the ground that the case-law stemming from the judgment of 30 May 2006, Parliament v Council and Commission, C-317/04 and C-318/04, EU:C:2006:346 (paragraphs 57 to 59), relating to the first indent of Article 3(2) of Directive 95/46, is applicable to that provision of the regulation.  
66      In that regard, it is true that, as previously held by the Court, the first indent of Article 3(2) of Directive 95/46, which was repealed and replaced by the GDPR with effect from 25 May 2018, generally excluded from its scope ‘processing operations concerning public security, defence [and] State security’, without drawing any distinction according the person carrying out the data processing operation concerned. Thus, processing operations carried out by private operators resulting from obligations imposed by the public authorities could, where appropriate, fall within the scope of the exception laid down in that provision, given that the wording of that provision covered all processing operations concerning public security, defence or State security, regardless of the person carrying out those operations (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 101).  
67      However, Article 2(2)(d) of the GDPR draws such a distinction, since, as noted by the Advocate General in points 41 and 46 of his Opinion, it is clearly apparent from the wording of that provision that two conditions need to be met for data processing to fall within the scope of the exception it lays down. While the first one of those conditions related to the purposes of the processing operation, namely, the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, the second condition relates to the person carrying out that operation, namely a ‘competent authority’ within the meaning of that provision.  
68      As the Court has also held, it is apparent from Article 23(1)(d) and (h) of the GDPR that the processing of personal data carried out by individuals for the purposes set out in Article 2(2)(d) of that regulation falls within the scope of thereof (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 102).  
69      It follows that the case-law stemming from the judgment of 30 May 2006, Parliament v Council and Commission (C-317/04 and C-318/04, EU:C:2006:346), relied on by the Belgian Government, is not applicable to the exception to the scope of the GDPR set out in Article 2(2)(d) thereof.  
70      In addition, that exception, like the other exceptions to the scope of the GDPR laid down in Article 2(2) of that regulation, must be interpreted strictly.  
71      As is apparent from recital 19 of the GDPR, the reason for that exception is that the processing of personal data by authorities competent for the purposes, inter alia, of the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security is governed by a more specific EU legal act, namely Directive 2016/680, which was adopted on the same day as the GDPR (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 69).  
72      As is stated, moreover, in recitals 9 to 11 of Directive 2016/680, the latter lays down the specific rules relating to the protection of natural persons with regard to such processing operations, respecting the specific nature of those activities in the fields of judicial cooperation in criminal matters and police cooperation, while the GDPR defines general rules concerning the protection of those persons which are intended to apply to those processing operations when Directive 2016/680, as a more specific legal act, does not apply. In particular, according to recital 11 of that directive, the GDPR applies to processing of personal data that is carried out by a ‘competent authority’ within the meaning of Article 3(7) of the said directive, but for purposes other than those of that directive (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 70).  
73      As regards the first condition set out in paragraph 67 above, and, specifically, the purposes for which the personal data are to be processed under the PNR Directive, it is appropriate to recall that, in accordance with Article 1(2) of that directive, PNR data may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Those purposes are covered by those set out in Article 2(2)(d) of the GDPR and Article 1(1) of Directive 2016/680, with the result that such processing operations may be caught by the exception laid down in Article 2(2)(d) of that regulation and, consequently, be within the scope of that directive.  
74      By contrast, that is not the case with regard to the processing operations covered by the API Directive and Directive 2010/65, the purposes of which are other than those in Article 2(2)(d) of the GDPR and Article 1(1) of Directive 2016/680.  
75      Indeed, the API Directive aims at improving border controls and combating illegal immigration, as is apparent from recitals 1, 7 and 9 as well as Article 1 thereof, by the transmission of advance passenger data by carriers to the competent national authorities. Moreover, several recitals and provisions of that directive make clear that the data processing operations envisaged for its implementation are within the scope of the GDPR. Recital 12 of that directive states that ‘Directive [95/46] applies with regard to the processing of personal data by the authorities of the Member States’. In addition, the fifth subparagraph of Article 6(1) of the API Directive specifies that Member States may also use API data for law enforcement purposes, ‘subject to data protection provisions under Directive [95/46]’, that phrase being used also in the third subparagraph of that provision. Similarly, the phrase ‘without prejudice to the provisions of Directive [95/46]’ is used, inter alia, in recital 9 of the API Directive. Article 6(2) of the API Directive provides, lastly, that passengers must be informed by carriers ‘in accordance with the provisions laid down in Directive [95/46]’.  
76      As to Directive 2010/65, it follows from recital 2 and Article 1(1) thereof that the purpose of that directive is to simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard and by rationalising reporting formalities, for the facilitation of maritime transport, and in order to reduce the administrative burden for shipping companies. Article 8(2) of the said directive confirms that the data processing operations envisaged for its implementation fall within the scope of the GDPR, since that provision require Member States, concerning personal data, to ensure compliance with Directive 95/46.  
77      It follows that the data processing operations envisaged by national legislation transposing, into domestic law, the provisions of the API Directive and of Directive 2010/65 are within the scope of the GDPR. By contrast, data processing operations envisaged by national legislation that transpose, into domestic law, the PNR Directive may, pursuant to the exception in Article 2(2)(d) of that regulation, fall outside the scope of the regulation, subject to compliance with the second condition recalled in paragraph 67 above, namely that the person carrying out the processing operations is a competent authority within the meaning of the latter provision.  
78      As regards that second condition, the Court has held that, in so far as Directive 2016/680 defines, in Article 3(7) thereof, the concept of ‘competent authority’, such a definition must be applied, by analogy, to Article 2(2)(d) of the GDPR (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 69).  
79      Pursuant to Articles 4 and 7 of the PNR Directive, each Member State must, respectively, designate, as its PIU, an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime and adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU, the latter authorities being also competent for those purposes, as specified in Article 7(2) of that directive.  
80      It follows therefrom that the processing of PNR data by the PIU and the said competent authorities for such purposes satisfy both conditions referred to in paragraph 67 above, with the result that those operations are covered by the provisions of the PNR Directive itself as well as those of Directive 2016/680 and not those of the GDPR, as confirmed, moreover, by recital 27 of the PNR Directive.  
81      By contrast, since economic operators such as air carriers, although they have a legal obligation to transfer PNR data, are neither in charge of exercising public authority nor entrusted with public powers by that directive, they cannot be regarded as being competent authorities within the meaning of Article 3(7) of Directive 2016/680 and Article 2(2)(d) of the GDPR, with the result that the collection of those data and transfer to the PIU, by air carriers, are covered by that regulation. The same applies in a situation, such as that provided for by the Law of 25 December 2016, where the collection and transfer of the said data are operated by other carriers or by tour operators.  
82      The referring, lastly, raises the question of the impact, if any, of the adoption of national legislation intended to transpose the provisions of the PNR Directive, those of the API Directive and also those of Directive 2010/65, such as the Law of 25 December 2016. In that regard, it should be borne in mind that, as is apparent from paragraphs 72 and 75 to 77 above, the data processing operations provided for under those last two directives fall within the scope of the GDPR, which entails general rules on the protection of natural persons with regard to the processing of personal data.  
83      Thus, when a data processing operation carried out on the basis of that legislation is covered by the API Directive and/or Directive 2010/65, the GDPR applies to that operation. The same is true of a data processing operation carried out on that same basis and, in terms of its purpose and in addition to the PNR Directive, falls within the API Directive and/or Directive 2010/65. Lastly, when a data processing operation carried out on the basis of that same legislation, in terms of its purpose, falls outside the PNR Directive, the GDPR applies if the operation relates to the collection of PNR data and transfer to the PIU, by air carriers. By contrast, where such a processing operation is carried out by the PIU or the authorities competent for the purposes referred to in Article 1(2) of the PNR Directive, that operation is covered by Directive 2016/680, in addition to national law.  
84      In the light of the foregoing, the answer to Question 1 is that Article 2(2)(d) and Article 23 of the GDPR must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of the API Directive, those of Directive 2010/65 and also those of the PNR Directive in respect of, on the one hand, data processing operations carried out by private operators and, on the other hand, data processing operations carried out by public authorities covered, solely or in addition, by the API Directive or Directive 2010/65. By contrast, the said regulation does not apply to the data processing operations envisaged by such legislation which are covered only by the PNR Directive and are carried out by the PIU or by the authorities competent for the purposes referred to in Article 1(2) of that directive.  
B.        
Questions 2 to 4 and Question 6  
85      By its Questions 2 to 4 and Question 6, which it is appropriate to consider together, the referring court asks the Court, in essence, whether the PNR Directive is valid in the light of Articles 7 and 8 as well as Article 52(1) of the Charter. Those questions concern, inter alia:  
–        Annex I to that directive and the data listed in that annex, in particular those referred to in paragraphs 12 and 18 thereof, concerning the requirements for clarity and precision (Questions 2 and 3);  
–        Article 3(4) of the said directive and Annex I thereto, in that the system of generalised collection, transfer and processing of PNR data established by those provisions may apply to any person on a flight covered by the provisions of that directive (Question 4), and  
–        Article 6 of the PNR Directive in that it provides for advance assessment, by comparing PNR data against databases and/or processing them against pre-determined criteria, which applies to such data in a systematic and generalised manner, regardless of whether there is any objective ground for considering that the passengers concerned may present a risk to public security (Question 6).  
86      It should be noted as a preliminary point that, in accordance with a general principle of interpretation, an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter Thus, if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law (judgment of 2 February 2021,   
Consob  
, C-481/19, EU:C:2021:84, paragraph 50 and the case-law cited).  
87      In addition, it is settled case-law that, when a directive allows the Member States discretion to define transposition measures adapted to the various situations possible, they must, when implementing those measures, not only interpret their national law in a manner consistent with the directive in question but also ensure that they do not rely on an interpretation of the directive that would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles recognised by EU law (see, to that effect, judgments of 15 February 2016,   
N.  
, C-601/15 PPU, EU:C:2016:84, paragraph 60 and the case-law cited, and of 16 July 2020,   
État belge (Family reunification  
 – Minor child)  
, C-133/19, C-136/19 and C-137/19, EU:C:2020:577, paragraph 33 and the case-law cited).  
88      As regards the PNR Directive, it should be noted that recitals 15, 20, 22, 25, 36 and 37 thereof stress the importance that the EU legislature, by referring to the high level of data protection, gives to the full respect for fundamental rights enshrined in Articles 7, 8 and 21 of the Charter as well as the principle of proportionality, with the result that, as stated in recital 36, that directive ‘should … be implemented accordingly’.  
89      In particular, recital 22 of the PNR Directive points out that, ‘[by] taking fully into consideration the principles outlined in recent relevant case-law of the [Court], the application of th[at] Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality’ and ‘genuinely meet the objectives of necessity and proportionality in order to achieve the general interests recognised by the [European] Union and the need to protect the rights and freedoms of others in the fight against terrorist offences and serious crime’. That recital adds that that application ‘should be duly justified and the necessary safeguards put in place to ensure the lawfulness of any storage, analysis, transfer or use of PNR data’.  
90      Moreover, under Article 19(2) of the PNR Directive, the Commission, when reviewing the directive, must pay special attention to ‘compliance with the applicable standards of protection of personal data’, ‘the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in this Directive’ and ‘the length of the data retention period’.  
91      It is therefore appropriate to determine whether the PNR Directive, in accordance with, in particular, the requirements set out in its recitals and its provisions referred to in paragraphs 88 to 90 above, may be interpreted in a way that ensures full respect for the fundamental rights guaranteed in Articles 7 and 8 of the Charter as well as the principle of proportionality enshrined in Article 52(1) thereof.  
1.        
Interferences with the fundamental rights guaranteed in Articles 7 and 8 of the Charter resulting from the PNR Directive  
92      Article 7 of the Charter guarantees everyone the right to respect for his or her private and family life, home and communications, while Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her.  
93      As is apparent from Article 3(5) of the PNR Directive and the list in Annex I thereto, the PNR data covered by that directive include, inter alia, besides the name(s) of the air passenger(s), information necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers.  
94      Since the PNR data therefore include information on identified individuals, namely the air passengers concerned, the various forms of processing to which those data may be subject affect the fundamental right to respect for private life, guaranteed in Article 7 of the Charter (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraphs 121 and 122 and the case-law cited).  
95      Furthermore, the processing of PNR data such as that covered by the PNR Directive also falls within the scope of Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraph 123 and the case-law cited).  
96      It is settled case-law that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to those data with a view to their use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (Opinion 1/15,   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126 and the case-law cited).  
97      Thus, both the transfer of PNR data by air carriers to the PIU of the Member State concerned, provided for in Article 1(1)(a) of the PNR Directive, read in conjunction with Article 8 thereof, and the framework of conditions governing the retention of those data, their use and any further transfer to the competent authorities of that Member State, to the PIUs and the competent authorities of the other Member States, to Europol or to the authorities of third countries, which are permitted, inter alia, by Articles 6, 7, 9 and 10 to 12 of that directive, constitute interferences with the rights guaranteed in Articles 7 and 8 of the Charter.  
98      As regards the seriousness of those interferences, it should be noted, first, that according to Article 1(1)(a), read in conjunction with Article 8 thereof, the PNR Directive provides for the systematic and continuous transfer to the PIUs of PNR data relating to any air passenger on an extra-EU flight within the meaning of Article 3(2) of that directive, operated between third countries and the European Union. As noted by the Advocate General in point 73 of his Opinion, such a transfer involves general and full access, by the PIUs, to the PNR data disclosed, concerning all the persons using air transport services, irrespective of subsequent use of those data.  
99      Secondly, Article 2 of the PNR Directive provides, in paragraph 1 thereof, that Member States may decide to apply the directive to intra-EU flights within the meaning of Article 3(3) thereof, and specifies, in paragraph 2 thereof, that in that case all the provisions of the said directive ‘shall apply to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if they were PNR data from extra-EU flights’.  
100    Thirdly, even if some of the PNR data listed on Annex I to the PNR Directive, as summarised in paragraph 93 above, taken in isolation, do not appear to be liable to reveal precise information about the private life of the persons concerned, the fact remains that, taken as a whole, the data may, inter alia, reveal a complete travel itinerary, travel habits, relationships existing between one or more persons and the financial situation of air passengers, their dietary habits or state of health, and may even reveal sensitive information about those passengers (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, paragraph 128).  
101    Fourthly, under Article 6(2)(a) and (b) of the PNR Directive, the data transferred by air carriers are intended for advance assessment, prior to the passengers’ scheduled arrival or departure, as well as subsequent   
   
assessment.  
102    As regards advance assessment, it is apparent from Article 6(2)(a) and (3) of the PNR Directive that that assessment is carried out by the PIUs of the Member States, systematically and by automated means, that is to say continuously and regardless of whether there is any indication that there is a risk that the person concerned is involved in terrorist offences or serious crime. To that end, those provisions provide that PNR data may be compared against ‘relevant databases’ and be processed against ‘pre-determined’ criteria.  
103    Against this background, it should be borne in mind that the Court has already held that the extent of the interference which automated analyses of PNR data entail in respect of the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the pre-determined models and criteria and on the databases on which that type of data processing is based (Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraph 172).  
104    As noted by the Advocate General in point 78 of his Opinion, the processing operation provided for in Article 6(3)(a) of the PNR Directive, namely the comparison of PNR data against ‘relevant databases’, may provide additional information on the private lives of air passengers and may allow very precise conclusions to be drawn in that regard.  
105    As to the processing of PNR data against ‘pre-determined criteria’ provided for in Article 6(3)(b) of the PNR Directive, it is true that Article 6(4) of that directive requires that any assessment of passengers by those means must be carried out in a non-discriminatory manner and, in particular, should not be based on a series of characteristics referred to in the last sentence of that paragraph 4. In addition, the criteria used must be targeted, proportionate and specific.  
106    That being said, the Court has already held that, since automated analyses of PNR data are carried out on the basis of unverified personal data and are based on pre-determined models and criteria, they necessarily present some margin of error (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement  
)   
of 26 July 2017, EU:C:2017:592, paragraph 169). In particular, as noted, in essence, by the Advocate General in point 78 of his Opinion, it is apparent from Commission Working Document (SWD(2020) 128 final) annexed to its report of 24 July 2020 on the review of the PNR Directive that the number of positive matches from automated processing under Article 6(3)(a) and (b) of that directive which prove to be incorrect following individual review by non-automated means is fairly substantial, amounting in 2018 and 2019 to at least five out of six individuals identified. Those processing operations thus lead to a careful analysis of the PNR data relating to the said persons.  
107    As regards the subsequent assessment of PNR data provided for in Article 6(2)(b) of the PNR Directive, it is apparent from that provision that, during the period of six months after the transfer of the PNR data, referred to in Article 12(2) of that directive, the PIU is required, upon request from the competent authorities, to provide them with the PNR data and process those data in specific cases, for the purposes of combating terrorist offences and serious crime.  
108    In addition, even if, upon expiry of that period of six months, PNR data are depersonalised through masking out of certain data elements, the PIU may be required, pursuant to Article 12(3) of the PNR Directive, to disclose, following such a request, full PNR data in a form which permits the identification of the data subject by the competent authorities where it is reasonably believed that it is necessary for the purposes referred to Article 6(2)(b) of that directive, such disclosure being however subject to approval granted by a judicial authority or ‘another [competent] national authority’.  
109    Fifthly, by providing, in Article 12(1) thereof, without providing further details in that regard, that PNR data are to be retained in a database for a period of five years following their transfer to the PIU of the Member State on the territory of which the flight is landing or departing, the PNR Directive, given the fact that, despite being depersonalised upon expiry of the initial period of six months though masking out of certain data elements, full PNR data may still be disclosed in the scenario referred to in the preceding paragraph, makes it possible for information on the private life of air passengers to be available for a period of time which the Court, in its Opinion 1/15   
(EU-Canada PNR Agreement  
)   
of 26 July 2017 (EU:C:2017:592, paragraph 132), has already described as being particularly long.  
110    Given how common use of air transport services is, the effect of a retention period that long is that a very large part of the population of the European Union is liable to have its PNR data retained, repeatedly, under the system established by the PNR Directive and, accordingly, be accessible for analyses carried out in the context of advance and subsequent assessments by the PIU and competent authorities over a considerable – even indefinite – period of time, in the case of persons who travel by air more than once every five years.  
111    In the light of all of the foregoing, it is appropriate to find that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so far, inter alia, as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services.  
2.        
Justification for the interferences resulting from the PNR Directive  
112    It must be borne in mind that the fundamental rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (Opinion 1/15   
(EU-Canada PNR Agreement  
)   
of 26 July 2017, EU:C:2017:592, paragraph 136 and the case-law cited, and judgment of 6 October 2020,   
Privacy International  
, C-623/17, EU:C:2020:790, paragraph 63 and the case-law cited).  
113    Under the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. In this connection, Article 8(2) of the Charter states that personal data must, inter alia, be processed ‘for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.  
114    It should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned, bearing in mind, on the one hand, that that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances (see, to that effect, judgment of 26 April 2022,   
Poland  
 v   
Parliament and Council  
, C-401/19, EU:C:2022:297, paragraphs 64 and 74 and the case-law cited) and, on the other hand, that the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter.  
115    As regards observance of the principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (Opinion 1/15   
(EU-Canada PNR Agreement  
)   
of 26 July 2017, EU:C:2017:592, paragraph 140, and judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others,  
 C-140/20,   
EU:C:2022:258  
, paragraph 52 and the case-law cited).  
116    More specifically, the question whether the Member States may justify a limitation on the rights guaranteed in Articles 7 and 8 of the Charter must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness (see, to that effect, judgments of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, paragraph 55 and the case-law cited, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 53 and the case-law cited).  
117    In order to satisfy the proportionality requirement, the legislation in question entailing the interference must lay down clear and precise rules governing the scope and application of the measures provided for and imposing minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subject to automated processing. Those considerations apply especially where the PNR data are liable to reveal sensitive passenger data (Opinion 1/15   
(EU-Canada PNR Agreement  
)   
of 26 July 2017, EU:C:2017:592, paragraph 141, and judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).  
118    Thus, legislation that provides for the retention of personal data must continue to satisfy objective criteria that establish a connection between the data to be retained and the objective pursued (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement  
)   
of 26 July 2017, EU:C:2017:592, paragraph 191 and the case-law cited, and judgments of 3 October 2019,   
A and Others  
, C-70/18, EU:C:2019:823, paragraph 63, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 133).  
(a)      
Observance of the principle of legality and respect for the essence of the fundamental rights in question  
119    Provision is made in an EU legislative act for the limitation of the exercise of the fundamental rights guaranteed in Articles 7 and 8 of the Charter stemming from the system established by the PNR Directive. As to the question whether, in accordance with the case-law referred to in paragraph 114 above, that directive, as an act of EU law which permits interference with those rights, itself defines the scope of the limitation on the exercise of the rights concerned, it must be noted that the provisions of the said directive as well as Annexes I and II thereto, first, list PNR data and, secondly, provide a framework for processing those data, inter alia, by laying down the purposes and detailed rules governing those processing operations. Moreover that question is largely the same as that of compliance with the proportionality requirement referred to in paragraph 117 above (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 180), and will be examined in paragraph 125 et seq. below.  
120    As regards respect for the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter, it is true that PNR data may, in some circumstances, reveal very specific information on the private life of a person. However, in so far as, on the one hand, the nature of that information is limited to certain aspects of a person’s private life, concerning that person’s air travel in particular, and, on the other hand, the PNR Directive expressly prohibits in Article 13(4) thereof the processing of sensitive data within the meaning of Article 9(1) of the GDPR, the data covered by that directive do not by themselves allow for a full overview of the private life of a person. In addition, that directive, in Article 1(2) thereof read in conjunction with Article 3(8) and (9) thereof as well as Annex II thereto, circumscribes the purposes for which those data are to be processed. Lastly, that same directive, in Articles 4 to 15 thereof, lays down the rules governing the transfer, processing and retention of those data as well as the rules intended to ensure, inter alia, the security, confidentiality and integrity of those data, and to protect them against unlawful access and processing. In those circumstances, the interferences which the PNR Directive entails do not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter.  
(b)      
Objective of general interest and appropriateness of the processing of PNR data having regard to that objective  
121    As to the question whether the system established by the PNR Directive pursues an objective of general interest, it is apparent from recitals 5, 6 and 15 of that directive that the objectives thereof are to ensure the internal security of the European Union and thus protect the life and safety of persons, while creating a legal framework that guarantees a high level of protection of passengers’ fundamental rights, in particular the right to the respect for private life and that of the protection of personal data, where PNR data are processed by the competent authorities.  
122    To that end, Article 1(2) of the PNR Directive provides that PNR data collected in accordance with that directive may be subject to the processing operations referred to in Article 6(2)(a) to (c) thereof only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Those purposes undoubtedly constitute objectives of general interest of the European Union that are capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter (see, to that effect, judgment of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 42, and Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017,   
EU:C:2017:592  
, paragraphs 148 and 149).  
123    As to the whether the system established by the PNR Directive is appropriate for the purpose of attaining the objectives pursued, it should be noted that while the possibility of ‘false negatives’ and the fairly substantial number of ‘false positives’ resulting, as noted in paragraph 106 above, from automated processing under that directive in 2018 and 2019, are liable to limit the appropriateness of that system, they are not capable, however, of rendering the said system inappropriate for the purpose of contributing to the attainment of the objective of combating terrorist offences and serious crime. As is apparent from the Commission working document referred to in paragraph 106 above, automated processing carried out under the said directive have indeed already made it possible to identify air passengers presenting a risk in the context of the fight against terrorist offences and serious crime.  
124    In addition, having regard to the margin of error inherent in the automated processing of PNR data and, in particular, the fairly substantial number of ‘false positives’, the appropriateness of the system established by the PNR Directive essentially depends on the proper functioning of the subsequent verification of the results obtained under those processing operations, by non-automated means, which, pursuant to that directive, is task for the PIU. The provisions laid down to that effect by the said directive thus contribute to the attainment of those objectives.  
(c)      
Whether the interferences from the PNR Directive are necessary  
125    According to the case-law recalled in paragraphs 115 to 118 above, it must be determined whether the interferences resulting from the PNR Directive are limited to what is strictly necessary and, inter alia, whether that directive lays down clear and precise rules governing the scope and application of the measures provided for and whether the system it establishes continues to meet objective criteria that establish a connection between PNR data, closely linked to booking for and engaging in air travel, and the objectives pursued by that directive, namely the fight against terrorist offences and serious crime.  
(1)      
Air passenger data covered by the PNR Directive  
126    It is necessary to assess whether the data headings in Annex I to the PNR Directive define in a clear and precise manner the PNR data which air carriers are required to provide to the PIU.  
127    As a preliminary point, it must be recalled that, as is apparent from recital 15 of the PNR Directive, the EU legislature intended for the list of the PNR data to be obtained by a PIU to be drawn up ‘with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the [European] Union as well as protecting the fundamental rights, in particular privacy and the protection of personal data’. In particular, under that same recital, those data ‘should only contain details of passengers’ reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security’. In addition, the PNR Directive prohibits, in the first sentence of Article 13(4) thereof, ‘the processing of PNR data revealing a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation’.  
128    Consequently, PNR data collected and provided in accordance with Annex I to the PNR Directive must relate directly to the flight operated and the passenger concerned and must be limited in such a way as to, on the one hand, meet solely the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime and, on the other, exclude sensitive data.   
129    Headings 1 to 4, 7, 9, 11, 15, 17 and 19 of Annex I to the PNR Directive meet those requirements as well as those of clarity and precision, in that they concern clearly identifiable and circumscribed information directly related to the flight operated and the passenger concerned. As noted by the Advocate General in point 165 of his Opinion, the same is true of headings 10, 13, 14 and 16, despite their ‘open-ended’ wording.   
130    However, clarifications are needed for the purposes of interpreting headings 5, 6, 8, 12 and 18.  
131    Heading 5, entitled ‘address and contact information (telephone number, email address)’, does not expressly specify whether the said address and contact information refer to the air passenger alone or also cover third parties who made the flight reservation for the air passenger, third parties through whom an air passenger may be contacted, or indeed third parties who are to be informed in the event of an emergency. However, as noted by the Advocate General, in essence, in point 162 of his Opinion, given the requirements of clarity and precision, that heading cannot be interpreted as allowing, implicitly, also the collection and transfer of personal data of such third parties. Consequently, that heading should be interpreted as referring only to the postal address and contact information, namely the telephone number and email address, of the air passenger on behalf of whom the reservation is made.   
132    As to heading 6, which relates to ‘all forms of payment information, including billing address’, that heading, in order to meet the requirements of clarity and precision, must be interpreted as covering solely information relating to the payment methods for, and billing of, the air ticket, to the exclusion of any other information not directly relating to the flight (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, paragraph 159).  
133    Heading 8, which relates to ‘frequent flyer information’, must be interpreted, as noted by the Advocate General in point 164 of his Opinion, as referring exclusively to data relating to the status of the passenger concerned in the context of a customer loyalty programme of a given airline or a given group of airlines as well as the number identifying that passenger as a ‘frequent flyer’. Heading 8 thus does not permit the collection of information relating to transactions through which that status was acquired.  
134    Heading 12 concerns ‘general remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)’.  
135    In that regard, it must be noted from the outset that whereas the phrase ‘general remarks’ does not meet the requirements of clarity and precision in that it does not set, as such, any limitation on the nature and scope of the information that may be collected and provided to a PIU under heading 12 (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, paragraph 160), the list in brackets does.  
136    Consequently, in order to interpret heading 12, in accordance with the case-law recalled in paragraph 86 above, in a manner that complies with the requirements of clarity and precision and, more generally, with Articles 7 and 8 as well as Article 52(1) of the Charter, it is appropriate to consider that only the collection and provision of information expressly listed under that heading are allowed, namely the name and gender of minor air passengers, their age, language(s) spoken, the name and contact details of the guardian on departure and relationship to the minor, the name and contact details of the guardian on arrival and relationship to the minor, departure and arrival agent.  
137    Lastly, heading 18 refers to ‘any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)’.  
138    As noted, in essence, by the Advocate General, in points 156 to 160 of his Opinion, it is apparent from that heading 18, read in the light of recitals 4 and 9 of the PNR Directive, that the information to which it refers is exhaustively the API data listed in the said heading as well as in Article 3(2) of the API Directive.  
139    Thus heading 18, in so far as it is construed as covering only the information expressly referred to in that heading and in Article 3(2) of the API Directive, may be regarded as meeting the requirements of clarity and precision (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraph 161).  
140    Accordingly, it must be held that, interpreted in accordance with the considerations set out inter alia in paragraphs 130 to 139 above, Annex I to the PNR Directive is of a sufficiently clear and precise nature overall, thus defining the scope of the interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter.  
(2)      
The purposes for which PNR data may be processed  
141    As is apparent from Article 1(2) of the PNR Directive, the PNR data collected in accordance with that directive are to be processed for the purposes of combating ‘terrorist offences’ and ‘serious crime’.  
142    As to whether the PNR Directive provides, in that context, for clear and precise rules that limit the application of the system established by that directive to what is strictly necessary for those purposes, it should be borne in mind, first, that the phrase ‘terrorist offences’ is defined in Article 3(8) of the said directive by reference to the ‘offences under national law referred to in Articles 1 to 4 of Framework Decision [2002/475]’.  
143    In addition to the fact that that framework decision, in Articles 1 to 3 thereof, defined in a clear and precise manner ‘terrorist offences’, ‘offences related to a terrorist group’ and ‘offences related to terrorist activities’, which Member States had to ensure were made punishable as criminal offences under that framework decision, Directive 2017/541, in Articles 3 to 14 thereof, also defines those same offences in a clear and precise manner.  
144    Secondly, Article 3(9) of the PNR Directive defines ‘serious crime’ by reference to the ‘offences listed in Annex II [to that directive] that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State’.  
145    However, first of all, that annex lists exhaustively the different categories of offences that might be covered by the notion of ‘serious crime’ referred to in Article 3(9) of the PNR Directive.  
146    Next, having regard to the particular features, at the time that directive was adopted, of the criminal justice systems of the Member States in the absence of harmonisation of the offences thus referred to, it was possible for the EU legislature merely to refer to categories of offences without defining the constitutive elements thereof, especially since those elements are necessarily defined under the national law to which Article 3(9) of the PNR Directive refers, in that Member States are bound by the respect for the principle of legality of criminal offences and penalties as a component of the common value, shared with the European Union, of the rule of law under Article 2 TEU (see, by analogy, judgment of 16 February 2022,   
Hungary  
 v   
Parliament and Council  
, C-156/21, EU:C:2022:97, paragraphs 136, 160 and 234), which principle is, moreover, is enshrined in Article 49(1) of the Charter, which Member States are required to observe when they implement an EU measure such as the PNR Directive (see, to that effect, judgment of 10 November 2011,   
QB  
, C-405/10, EU:C:2011:722, paragraph 48 and the case-law cited). Thus, in the light of the usual meaning of the terms used in that annex, it must be found that the said annex determines, in a sufficiently clear and precise manner, the offences that may constitute serious crime.   
147    It is true that paragraphs 7, 8, 10 and 16 of Annex II relate to categories of offences that are very general (fraud, laundering of the proceeds of crime and counterfeiting of currency, environmental crime, illicit trafficking in cultural goods) while nonetheless referring to specific offences falling within those general categories. In order to ensure the requisite level of precision under Article 49 of the Charter also, those paragraphs must be interpreted as referring to the said offences, as defined in the relevant area of national and/or EU law. When interpreted that way those paragraphs can be regarded as meeting the requirements of clarity and precision.   
148    Lastly, it is important also to bear in mind that, although, in accordance with the principle of proportionality, the objective of combating serious crime is capable of justifying the serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter which the PNR Directive entails, the same is not true of the objective of combating criminality in general, since the latter objective may justify solely non-serious interferences (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 59 and the case-law cited). Thus, that directive must ensure, by means of clear and precise rules, that the application of the system established by the said directive is limited to offences amounting to serious crime and thereby excludes those amounting to ordinary crime.   
149    In that regard, as noted by the Advocate General in point 121 of his Opinion, many of the offences listed in Annex II to the PNR Directive – such as human trafficking, the sexual exploitation of children and child pornography, illicit trafficking in weapons munitions and explosives, money laundering, cybercrime, illicit trade in human organs and tissue, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in nuclear or radioactive materials, unlawful seizure of aircraft/ships, serious crimes within the jurisdiction of the International Criminal Court, murder, rape, kidnapping, illegal restraint and hostage-taking – are inherently and indisputably extremely serious.  
150    In addition, although other offences, also referred to in that Annex II, are less likely, a priori, to be associated with serious crime, it is nevertheless apparent from Article 3(9) of the PNR Directive that those offences may be considered to amount to serious crime only if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of the Member State concerned. The requirements flowing from that provision, which relate to the nature and severity of the penalty applicable, are, in principle, such as to limit the application of the system established by that directive to offences that have the requisite level of seriousness to justify the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter stemming from the system established by the said directive.  
151    Nonetheless, since Article 3(9) of the PNR Directive refers to the maximum rather than the minimum penalty applicable, it cannot be ruled out that PNR data may be processed for the purposes of combating offences which, although meeting the criterion laid down by that provision relating to the threshold of severity, amount to ordinary crime rather than serious crime, having regard to the particular features of the domestic criminal justice system.  
152    It is thus for the Member States to ensure that the application of the system established by the PNR Directive is effectively limited to combating serious crime and that that system does not extend to offences that amount to ordinary crime.   
(3)      
The link between PNR data and the purposes for which those data are processed  
153    It is true that, as noted, in essence, by the Advocate General in point 119 of his Opinion, the wording of Article 3(8) and Article 3(9) of the PNR Directive, read in conjunction with Annex II thereto, does not expressly refer to a criterion that is capable of confining the scope of that directive solely to offences that may, by their nature, have an objective link, even if only indirect one, with air travel and, therefore, with the categories of data transferred, processed and retained pursuant to that directive.  
154    Nevertheless, as pointed out by the Advocate General in point 121 of his Opinion, certain offences listed in Annex II to the PNR Directive, such as human trafficking, illicit trafficking in narcotic drugs or weapons, facilitation of unauthorised entry and residence and the unlawful seizure of aircraft, are, by their very nature, likely to have a direct link with the carriage of passengers by air. The same is true of certain terrorist offences, such as causing extensive destruction to a transport system or an infrastructure facility or seizure of aircraft, offences under Article 1(1)(d) and (e) of Framework Decision 2002/475, to which Article 3(8) of the PNR Directive refers, or travelling for the purpose of terrorism and organising or otherwise facilitating such travelling, offences under Articles 9 and 10 of Directive 2017/541.  
155    Against that background, it must also be borne in mind that the Commission provided reasons for its Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime of 2 February 2011 (COM(2011) 32 final), which became the PNR Directive, emphasising the fact that ‘the terrorist attacks in the United States in 2001, the aborted terrorist attack in August 2006 aimed at blowing up a number of aircraft on their way from the United Kingdom to the United States, and the attempted terrorist attack on board a flight from Amsterdam to Detroit in December 2009 showed the ability of terrorists to mount attacks, targeting international flights, in any country’ and that ‘most terrorist activities are transnational in character and involve international travel, inter alia to training camps outside the [European Union]’. In addition, in order to justify the need for analysis of PNR data for the purposes of combating serious crime, the Commission referred, by way of example, to the case of a group of human traffickers who had used fake documents to check in for a flight as well as that of a human and drug trafficking network which, for the purposes of importing drugs to several destinations in Europe, had used persons who were themselves trafficked persons and had bought their air tickets with stolen credit cards. All of those cases concerned offences having a direct link with the carriage of passengers by air in that they were offences targeting the carriage of passengers by air as well as offences committed during or through travel by air.  
156    In addition, it is important to note that even offences that have no such direct link with the carriage of passengers by air may, depending on the circumstances of the case, have an indirect link with the carriage of passengers by air. Such is the case, in particular, when air transport is used as a means of preparing such offences or evading criminal prosecution after committing such offences. By contrast, offences having no objective link, not even an indirect one, with the carriage of passengers by air cannot justify the application of the system established by the PNR Directive.  
157    In those circumstances, Article 3(8) and (9) of that directive, read in conjunction with Annex II thereto and in the light of the requirements stemming from Articles 7 and 8 as well as Article 52(1) of the Charter, requires Member States, in particular upon individual review by non-automated means as referred to in Article 6(5) of that directive, to ensure that the application of the system established by it be limited to terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.   
(4)      
The air passengers and flights concerned  
158    The system established by the PNR Directive covers the PNR data of anyone who meets the definition of ‘passenger’ within the meaning of Article 3(4) of that directive on a flight falling within the scope thereof.   
159    According to Article 8(1) of the said directive, those data are transferred to the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart, regardless of whether there is any objective evidence from which it may be inferred that the passengers concerned may present a risk of being involved in a terrorist offence or serious crime. The data thus transferred are, inter alia, processed by automated means in connection with the advance assessment under Article 6(2)(a) and (3) of the PNR Directive, the objective of that assessment, as is apparent from recital 7 of that directive, being the identification of persons who were not suspected of involvement in terrorist offences or serious crime prior to that assessment and who should be subject to further examination by the competent authorities.  
160    Specifically, it is apparent from Article 1(1)(a) and Article 2 of the PNR Directive that the latter distinguishes between passengers of extra-EU flights, operated between the European Union and third countries, and those of intra-EU flights, operated between different Member States.  
161    As regards passengers of extra-EU flights, it must be recalled that, in respect of passengers flying between the European Union and Canada, the Court has already held that the automated processing of their PNR data, before their arrival in Canada, facilitates and expedites security checks, in particular at borders. Furthermore, the exclusion of certain categories of persons, or of certain areas of origin, would be liable to prevent the achievement of the objective of automated processing of PNR data, namely identifying, through verification of that data, persons liable to present a risk to public security from amongst all air passengers, and make it possible for that verification to be circumvented (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraph 187).  
162    Those considerations can be applied   
mutatis mutandis  
 to the situation of passengers flying between the European Union and all third countries, whom Member States are required to subject to the system established by the PNR Directive pursuant to Article 1(1)(a) of that directive, read in conjunction with Article 3(2) and (4) of the said directive. The transfer and advance assessment of the PNR data of air passengers entering or leaving the European Union cannot be restricted to a particular group of air passengers, given the very nature of the threats to public security that may stem from terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air between the European Union and third countries. Thus, it must be found that the necessary connection between those data and the objective of combating such offences exists, with the result that the PNR Directive does not go beyond what is strictly necessary merely because it imposes on Member States the systematic transfer and advance assessment of the PNR data of all those passengers.  
163    As regards passengers flying between different Member States of the European Union, Article 2(1) of the PNR Directive, read in conjunction with recital 10 thereof, provides only that Member States may extend the application of the system established by that directive to intra-EU flights.  
164    Thus, the EU legislature did not intend to oblige Member States to extend the application of the system established by the PNR Directive to intra-EU flights but, as is apparent from Article 19(3) of that directive, reserved its decision concerning such an extension, while taking the view that it should be preceded by a detailed assessment of the legal implications thereof, in particular for the fundamental rights of the data subjects.   
165    In that regard, it should be noted that, by stating that the Commission’s review report referred to in Article 19(1) of the PNR Directive must ‘also include a review of the necessity, proportionality, and effectiveness of including within the scope of th[at] Directive the mandatory collection and transfer of PNR data relating to all or selected intra-EU flights’ and that it must, in that regard, take into account ‘the experience gained by Member States, especially those Member States that apply th[at] Directive to intra-EU flights in accordance with Article 2’, Article 19(3) of that directive makes apparent that, for the EU legislature, the system established by the said directive must not necessarily extend to all intra-EU flights.   
166    In a similar vein, Article 2(3) of the PNR Directive provides that Member States may decide to apply that directive only to selected intra-EU flights when they consider it necessary in order to pursue the objectives of the said directive, while being able to change the selected flights at any time.  
167    In any event, the Member States’ power to extend the application of the system established by the PNR Directive to intra-EU flights is to be exercised, as is apparent from recital 22 thereof, in full respect for the fundamental rights guaranteed in Articles 7 and 8 of the Charter. In that regard, while, according to recital 19 of the directive, it is for the Member States to assess the threats linked to terrorist offences and serious crime, the fact remains that the exercise of that power presupposes that, upon that assessment, Member States find that there is a threat related to those offences which is capable of justifying the application of the said directive to intra-EU flights also.   
168    In those circumstances, a Member State, when it wishes to exercise the power provided for in Article 2 of the PNR Directive, either for all intra-EU flights under paragraph 2 of that article or only for such selected flights under paragraph 3 of the said article, is not exempt from the requirement to verify that the extension of the application of that directive to selected or all intra-EU flights is effectively necessary and proportionate for the purposes of attaining the objective set out in Article 1(2) of the said directive.   
169    Thus, given recitals 5 to 7, 10 and 22 of the PNR Directive, the Member State must verify that the processing, under that directive, of the PNR data of passengers of intra-EU flights or selected such flights is strictly necessary, having regard to the seriousness of the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, in order to ensure the internal security of the European Union or, at least, that of that Member State and, thus, protect the life and safety of persons.   
170    As regards, in particular, the threats related to terrorist offences, it is apparent from the Court’s case-law that terrorist activities are amongst those capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, particularly, of directly threatening society, the population or the State itself, and that it is of paramount interest for each Member State to prevent and punish those activities to protect the essential functions of the State and the fundamental interests of society in order to safeguard national security. Such threats are distinguishable, by their nature, their particular seriousness and the specific nature of the circumstances of which they are constituted, from the general and permanent risk of serious criminal offences being committed (see, to that effect, judgments of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 and 136, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraphs 61 and 62).  
171    Thus, in a situation where it is established, on the basis of the assessment carried out by a Member State, that there are sufficiently solid grounds for considering that the latter is confronted with a terrorist threat which is shown to be genuine and present or foreseeable, the fact that that Member State makes provision for the application of the PNR Directive, pursuant to Article 2(1) of that directive, to all intra-EU flights from or to the said Member State, for a limited period of time, does not appear to go beyond what is strictly necessary. The existence of that threat is, in itself, capable of establishing a connection between, on the one hand, the transfer and processing of the data concerned and, on the other, the fight against terrorism (see, by analogy, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 137).  
172    The decision providing for that application must be open to effective review, either by a court or by an independent administrative body whose decision is binding, in order to verify that that situation exists and that the conditions and safeguards which must be laid down are observed. The period of application must also be limited in time to what is strictly necessary but may be extended if that threat persists (see, by analogy, judgments of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 58).  
173    By contrast, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, the indiscriminate application by that Member State of the system established by the PNR Directive not only to extra-EU flights but also to all intra-EU flights would not be considered to be limited to what is strictly necessary.   
174    In such a situation, the application of the system established by the PNR Directive to selected intra-EU flights must be limited to the transfer and processing of the PNR data of flights relating, inter alia, to certain routes or travel patterns or to certain airports in respect of which there are indications that are such as to justify that application. It is for the Member State concerned, in that situation, to select the intra-EU flights, according to the outcome of the assessment which it must carry out on the basis of the requirements set out in paragraphs 163 to 169 above, and to review that assessment regularly in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of the system established by that directive to intra-EU flights continues to be limited to what is strictly necessary.  
175    It follows from the foregoing that the interpretation, thus followed, of Article 2 and Article 3(4) of the PNR Directive, in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, is capable of ensuring that those provisions are within the limits of what is strictly necessary.  
(5)      
Advance assessment of PNR data by automated processing  
176    Under Article 6(2)(a) of the PNR Directive, the objective of the advance assessment provided for therein is to identify persons who require further examination, inter alia by the competent authorities referred to in Article 7 of that directive, in view of the fact that such persons may be involved in a terrorist offence or serious crime.   
177    That advance assessment is carried out in two stages. As a first step, the PIU of the Member State concerned, pursuant to Article 6(3) of the PNR Directive, processes PNR data by automated means by comparing them against databases or pre-determined criteria. As a second step, should that processing by automated means lead to a positive match (‘hit’), that unit, pursuant to Article 6(5) of the said directive, is to carry out an individual review by non-automated means to verify whether the competent authorities referred to in Article 7 of the said directive need to take action under national law (‘match’).  
178    As recalled in paragraph 106 above, automated processing necessarily presents a fairly substantial margin of error, since it is carried out on the basis of unverified personal data and is based on pre-determined criteria.   
179    In those circumstances, and given the need, highlighted in the fourth recital of the preamble to the Charter, to strengthen the protection of fundamental rights in the light, inter alia, of scientific and technological developments, it must be ensured, as stated in recital 20 and Article 7(6) of the PNR Directive, that no decision that produces an adverse legal effect on a person or significantly affects a person may be taken by the competent authorities only by reason of the automated processing of PNR data. Moreover, in accordance with Article 6(6) of that directive, the PIU itself may transfer PNR data to those authorities only after individual review by non-automated means. Lastly, in addition to those verifications which the PIU and the competent authorities are to carry out themselves, the lawfulness of all automated processing must be open to review by the data protection officer and the national supervisory authority, in accordance with Article 6(7) and Article 15(3)(b), respectively, of that directive as well as by the national courts in the context of the judicial redress referred to in Article 13(1) of that same directive.  
180    As noted, in essence, by the Advocate General in point 207 of his Opinion, the national supervisory authority, the data protection officer and the PIU must be provided with the material and human resources necessary to carry out their review under the PNR Directive. Furthermore, it is important that the national legislation transposing that directive into domestic law and authorising the automated processing provided for by the directive lays down clear and precise rules for the determination of the databases and criteria for analysis used, without relying, for the purposes of advance assessment, on other methods not referred to expressly in Article 6(2) of that directive.  
181    Moreover, it follows from Article 6(9) of the PNR Directive that the consequences of advance assessment under Article 6(2)(a) thereof do not jeopardise the right of entry of persons enjoying the right of free movement within the territory of the Member State concerned as laid down in Directive 2004/38 and must, also, comply with Regulation No 562/2006. Thus, the system established by the PNR Directive does not allow the competent authorities to limit that right beyond what is prescribed by Directive 2004/38 and Regulation No 562/2006.  
(i)      
Comparing PNR data against databases  
182    Under Article 6(3)(a) of the PNR Directive, the PIU ‘may’, when carrying out the assessment referred to in Article 6(2)(a) of that directive, compare PNR data against ‘[relevant] databases’ for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, ‘including databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases’.   
183    Although it follows from the very wording of that Article 6(3)(a) of the PNR Directive, in particular from the word ‘including’, that the databases on persons or objects sought or under alert are among the ‘relevant databases’ referred to in that provision, that provision does not specify which other databases could also be considered to be ‘relevant’ in the light of the objectives pursued by that directive. As noted by the Advocate General in point 217 of his Opinion, that provision does not expressly indicate the nature of the data that those databases may contain or their relationship to those objectives nor does it mention whether PNR data must be compared exclusively against databases managed by public authorities or whether they may also be compared against databases managed by private individuals.   
184    In those circumstances, Article 6(3)(a) of the PNR Directive could, prima facie, lend itself to an interpretation according to which PNR data may be used as mere search criteria for the purposes of conducting analyses using various databases, including databases managed and exploited by the security and intelligence agencies of Member States in order to pursue objectives other than those referred to in that directive, and that those analyses may take the form of ‘data mining’. The fact that such analyses can be conducted and PNR data compared to such databases may give rise in the minds of passengers of carriage by air to the feeling that their private life is under a form of surveillance. Thus, while the advance assessment provided for in that provision relies on a relatively limited set of PNR data, such an interpretation of that Article 6(3)(a) cannot be adopted, since it would lead to a disproportionate use of those data providing the means of establishing a detailed profile of the individuals concerned solely because they intend to travel by air.  
185    Therefore, according to the case-law recalled in paragraphs 86 and 87 above, Article 6(3)(a) of the PNR Directive must be interpreted in such a way as to ensure full respect for the fundamental rights enshrined in Articles 7 and 8 of the Charter.   
186    In that regard, it is apparent from recitals 7 and 15 of the PNR Directive that the automated processing provided for in Article 6(3)(a) of that directive must be limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime, while ensuring a high level of protection of those fundamental rights.  
187    In addition, as observed, in essence, by the Commission in response to a question put by the Court, the wording of that provision, that the PIU ‘may’ compare PNR data against the databases referred to therein, allows the PIU to choose a processing method that is limited to what is strictly necessary, depending on the particular situation. In the light of the obligation to comply with the requirements of clarity and precision necessary to ensure the protection of the fundamental rights enshrined in Articles 7 and 8 of the Charter, the PIU must limit the automated processing provided for in Article 6(3)(a) of the PNR Directive to the databases identifiable under that provision. In that regard, whereas the reference, in the latter provision, to ‘relevant databases’ does not lend itself to an interpretation defining in a sufficiently clear and precise manner the databases thus referred to, the same is not true of the reference to ‘databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases’.  
188    Accordingly, as noted, in essence, by the Advocate General in point 219 of his Opinion, Article 6(3)(a) of the PNR Directive must, in the light of those fundamental rights, be interpreted as meaning that the latter databases are the only databases against which the PIU may compare PNR data.  
189    As regards the requirements which those databases must satisfy, it is appropriate to note that, under Article 6(4) of the PNR Directive, advance assessment against pre-determined criteria must, pursuant to Article 6(3)(b) of that directive, be carried out in a non-discriminatory manner, those criteria must be targeted, proportionate and specific, and must be set and regularly reviewed by the PIUs in cooperation with the competent authorities referred to in Article 7 of the directive. If, by referring to Article 6(3)(b) of that directive, the wording of Article 6(4) thereof covers only the processing of PNR data against pre-determined criteria, the latter provision must be interpreted, in the light of Articles 7, 8 and 21 of the Charter, as meaning that the requirements it lays down apply   
mutatis mutandis  
 to the comparison of those data against the databases referred in the preceding paragraph, especially since those requirements correspond, in essence, to those adopted by the case-law arising from Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017 (EU:C:2017:592, paragraph 172), for the purposes of cross-checking PNR data against databases.  
190    In that regard, it should be stated that the requirement as to the non-discriminatory nature of those databases implies, inter alia, that entry into the databases on persons sought or under alert is based on objective and non-discriminatory factors, defined in EU, international and national rules applicable to such databases (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 78).   
191    In addition, in order to satisfy the requirement as to the targeted, proportionate and specific nature of the pre-determined criteria, the databases referred to in paragraph 188 above must be used in relation to the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.   
192    Moreover, the databases used pursuant to Article 6(3)(a) of the PNR Directive must, in view of the considerations set out in paragraphs 183 and 184 above, be managed by the competent authorities referred to in Article 7 of that directive or, with regard to EU databases as well as international databases, be exploited by those authorities in the context of their mission to combat terrorist offences and serious crime. That is the case of the databases on persons or objects sought or under alert, in accordance with the EU, international and national rules applicable to such databases.   
(ii)   
Processing PNR data against pre-determined criteria  
193    Article 6(3)(b) of the PNR Directive provides that the PIU may also process PNR data against pre-determined criteria. As is apparent from Article 6(2)(a) of that directive, the advance assessment and, accordingly, the processing of PNR data against pre-determined criteria is intended, in essence, to identify persons who may be involved in a terrorist offence or serious crime.  
194    As regards the criteria that the PIU may use to that end, it should be noted, first, that according to the very wording of Article 6(3)(b) of the PNR Directive those must be ‘pre-determined’ criteria. As noted by the Advocate General in point 228 of his Opinion, that requirement precludes the use of artificial intelligence technology in self-learning systems (‘machine learning’), capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria.   
195    It is important to add that use of such technology would be liable to render redundant the individual review of positive matches and monitoring of lawfulness required by the provisions of the PNR Directive. As observed, in essence, by the Advocate General in point 228 of his Opinion, given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter, for which the PNR Directive, according to recital 28 thereof, seeks to ensure a high level of protection, in particular in order to challenge the non-discriminatory nature of the results obtained.  
196    Concerning, next, the requirements flowing from Article 6(4) of the PNR Directive, that provision states, in its first sentence, that any advance assessment against pre-determined criteria is to be carried out in a non-discriminatory manner and indicates, in its fourth sentence, that those criteria are in no circumstances to be based on a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.   
197    Thus Member States cannot use, as pre-determined criteria, criteria that are based on the characteristics referred to in the preceding paragraph and use of which may result in discrimination. In that regard, it follows from the wording of the fourth sentence of Article 6(4) of the PNR Directive, according to which pre-determined criteria are ‘in no circumstances’ to be based on those characteristics, that that provision covers both direct and indirect discrimination. That interpretation is, moreover, confirmed by Article 21(1) of the Charter, in the light of which the said provision must be read, which prohibits ‘any’ discrimination based on the said characteristics. In those circumstances, pre-determined criteria must be defined in such a way that, while worded in a neutral fashion, their application does not place persons having the protected characteristics at a particular disadvantage.  
198    As to the requirements relating to the targeted, proportionate and specific nature of pre-determined criteria, referred to in the second sentence of Article 6(4) of the PNR Directive, it follows from those requirements that the criteria used for the purposes of advance assessment must be determined in such a way as to target, specifically, individuals who might be reasonably suspected of involvement in terrorist offences or serious crime covered by that directive. That reading is supported by the very wording of Article 6(2)(a) thereof, which emphasises the ‘fact’ that the persons concerned ‘may’ be involved in ‘a’ terrorist offence or serious crime. In the same vein, recital 7 of the said directive states that the creation and application of assessment criteria should be limited to terrorist offences and serious crime ‘for which the use of such criteria is relevant’.  
199    In order to target in that way the persons thus referred to and given the risk of discrimination that criteria based on the characteristics set out in the fourth sentence of Article 6(4) of the PNR Directive entail, the PIU and the competent authorities cannot, generally, rely on those characteristics. By contrast, as pointed out by the German Government at the hearing, they can inter alia take into consideration specific features in the factual conduct of persons when preparing and engaging in air travel which, following the findings of and experience acquired by the competent authorities, might suggest that the persons acting in that way may be involved in terrorist offences or serious crime.   
200    In that context, as noted by the Commission in response to a question put by the Court, pre-determined criteria must be defined in such a way as to take into consideration both ‘incriminating’ as well as ‘exonerating’ circumstances, since that requirement may contribute to the reliability of those criteria and, in particular, ensure that they are proportionate, as required by the second sentence Article 6(4) of the PNR Directive.   
201    Lastly, the third sentence of Article 6(4) of that directive provides that pre-determined criteria must be reviewed regularly. In the context of that review, those criteria must be updated in accordance with changes in the circumstances that justified their being taken into consideration for the purposes of advance assessment, thus making it possible, inter alia, to react to developments in the fight against terrorist offences and serious crime referred to in paragraph 157 above (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 82). In particular, that review must take into account the experience acquired in the context of the application of pre-determined criteria, in order to reduce, as much as possible, the number of ‘false positives’ and, thereby, contribute to the strictly necessary nature of the application of those criteria.  
(iii)   
Safeguards surrounding the automated processing of PNR data  
202    Compliance with the requirements to which the automated processing of PNR data is subject under Article 6(4) of the PNR Directive is required not only when determining and reviewing the databases as well as the pre-determined criteria provided for in that provision, but also, as noted by the Advocate General in point 230 of his Opinion, throughout the process of processing those data.   
203    As regards pre-determined criteria specifically, it is appropriate, first of all, to specify that, although the PIU, as stated in recital 7 of the PNR Directive, must define the assessment criteria in a manner which keeps to a minimum the number of innocent people wrongly identified by the system established by that directive, that unit must still, in accordance with Article 6(5) and (6) of the said directive, individually review any positive match by non-automated means in order to identify, as much as possible, any ‘false positives’. In addition, notwithstanding the fact that they must set the assessment criteria in a non-discriminatory manner, the PIU is required to carry out such a review for the purposes of excluding any discriminatory results. The PIU must comply with that same review obligation when comparing PNR data against databases.  
204    Thus, the PIU must refrain from transferring the results of those automated processing operations to the competent authorities referred to Article 7 of the PNR Directive when, having regard to the considerations set out in paragraph 198 above, they do not, following that review, have anything capable of giving rise, to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime in respect of the persons identified by means of those automated processing operations or when they have reason to believe that those processing operations lead to discriminatory results.  
205    As regards the verifications which the PIU must carry out to that end, it follows from Article 6(5) and (6) of the PNR Directive, read in conjunction with recitals 20 and 22 thereof, that Member States must lay down clear and precise rules capable of providing guidance and support for the analysis carried out by the agents in charge of the individual review, for the purposes of ensuring full respect for the fundamental rights enshrined in Articles 7, 8 and 21 of the Charter and, in particular, guarantee a uniform administrative practice within the PIU that observes the principle of non-discrimination.  
206    In particular, given the fairly substantial number of ‘false positives’, mentioned in paragraph 106 above, Member States must ensure that the PIU establishes, in a clear and precise manner, objective review criteria enabling its agents to verify, on the one hand, whether and to what extent a positive match (‘hit’) concerns effectively an individual who may be involved in the terrorist offences or serious crime referred to in paragraph 157 above and must, therefore, be subject to further examination by the competent authorities referred to Article 7 of that directive, as well as, on the other hand, the non-discriminatory nature of automated processing operations under that directive and, in particular, the pre-determined criteria and databases used.  
207    In that context, Member States are required to ensure that, in accordance with Article 13(5) of the PNR Directive, read in conjunction with recital 37 thereof, the PIUs maintain documentation relating to all processing of PNR data carried out in connection with the advance assessment, including in the context of the individual review by non-automated means, for the purpose of verifying its lawfulness and for the purpose of self-monitoring.  
208    Next, the competent authorities, pursuant to the first sentence of Article 7(6) of the PNR Directive, cannot take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data, which means, in connection with the advance assessment, that they must take into consideration and, where applicable, give preference to the result of the individual review conducted by non-automated means by the PIU over that obtained by automated processing. The second sentence of that Article 7(6) specifies that those decisions must not be discriminatory.   
209    In that context, the competent authorities must ensure the lawfulness of the automated processing, in particular its non-discriminatory nature, as well as that of the individual review.  
210    In particular, the competent authorities must ensure that the person concerned – without necessarily allowing that person, during the administrative procedure, to become aware of the pre-determined assessment criteria and programs applying those criteria – is able to understand how those criteria and those programs work, so that it is possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress guaranteed in Article 13(1) of the PNR Directive, in order to call in question, as the case may be, the unlawful and, inter alia, discriminatory nature of the said criteria (see, by analogy, judgment of 24 November 2020,   
Minister van Buitenlandse Zaken  
, C-225/19 and C-226/19, EU:C:2020:951, paragraph 43 and the case-law cited). The same must apply to the review criteria mentioned in paragraph 206 above.  
211    Lastly, in the context of redress introduced pursuant to Article 13(1) of the PNR Directive, the court responsible for reviewing the legality of the decision adopted by the competent authorities as well as, except in the case of threats to State security, the persons concerned themselves must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken (see, by analogy, judgment of 4 June 2013,   
ZZ  
, C-300/11, EU:C:2013:363, paragraphs 54 to 59), including the pre-determined assessment criteria and the operation of the programs applying those criteria.  
212    Moreover, according to Article 6(7) and Article 15(3)(b), respectively, of the PNR Directive, it is for the data protection officer and the national supervisory authority to ensure the monitoring of the lawfulness of the automated processing carried out by the PIU in connection with the advance assessment, monitoring which covers, inter alia, whether those operations are not discriminatory. While the first of those provisions states, to that end, that the data protection officer has access to all data processed by the PIU, that access must necessarily cover the pre-determined criteria and databases used by that unit in order to guarantee effectivenes and a high level of data protection that that officer must ensure in accordance with recital 37 of that directive. Similarly, the investigations, inspections and audits that the national supervisory authority conducts pursuant to the second of those provisions may also concern those pre-determined criteria and those databases.  
213    It follows from all of the foregoing that the provisions of the PNR Directive governing the advance assessment of PNR data under Article 6(2)(a) of that directive lend themselves to an interpretation that is consistent with Articles 7, 8 and 21 of the Charter and comes within the limits of what is strictly necessary.   
(6)      
The disclosure and subsequent assessment of PNR data  
214    According to Article 6(2)(b) of the PNR Directive, PNR data may also, on request of the competent authorities, be provided to the latter and assessed subsequently to the scheduled arrival in or departure from the Member State.   
215    As regards the circumstances in which that disclosure and assessment may occur, it is apparent from the wording of that provision that the PIU may process PNR data in order to respond ‘on a case-by-case basis’ to ‘a duly reasoned request based on sufficient grounds’ from the competent authorities to have those data disclosed to them and processed ‘in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime’. In addition, where a request is introduced more than six months after the transfer of the PNR data to the PIU, a period upon the expiry of which the PNR data are depersonalised through masking out of certain elements, pursuant to Article 12(2) of that directive, Article 12(3) of the said directive provides that disclosure of the full PNR data and, therefore, a non-depersonalised version thereof, is permitted only under the dual condition that, first, it is reasonably believed that it is necessary for the purposes referred to in Article 6(2)(b) of the said directive and, secondly, it is approved by a judicial authority or another national authority competent under national law.   
216    In that regard, it is apparent, first of all, from the very wording of Article 6(2)(b) of the PNR Directive that the PIU cannot systematically proceed to the subsequent disclosure and assessment of the PNR data of all air passengers and that it can only respond ‘on a case-by-case basis’ to requests relating to such processing operations ‘in specific cases’. Having said that, in so far as that provision referred to ‘specific cases’, those processing operations must not necessarily be limited to the PNR data of a single air passenger but may, as noted by the Commission in response to a question put by the Court, also concern groups of persons provided that the persons concerned share a certain number of characteristics allowing them to be considered to constitute together a ‘specific case’ for the purposes of the intended data disclosure and assessment.  
217    Concerning, next, the substantive conditions required for the PNR data of air passengers to be disclosed and assessed subsequently, although Article 6(2)(b) and Article 12(3)(a) of the PNR Directive use ‘sufficient grounds’ and ‘reasonably’, respectively, without expressly specifying the nature of such grounds, it nonetheless follows from the very wording of the first of those provisions, which refers to the purposes mentioned in Article 1(2) of the said directive, that PNR data can be disclosed and assessed subsequently only in order to verify whether there are indications that the data subject may be involved in terrorist offences or serious crime having, as follows from paragraph 157 above, an objective link, even if only an indirect one, with the carriage of passengers by air.  
218    In the context of the system established by the PNR Directive, the disclosure and processing of PNR data under Article 6(2)(b) of that directive concern the data of persons who have already been subject to advance assessment prior to their scheduled arrival in or departure from the Member State concerned. In addition, a request for subsequent assessment may relate, inter alia, to persons whose PNR data have not been transferred to the competent authorities following an advance assessment, in so far as the latter has revealed nothing to suggest that those persons may be involved in terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air. In those circumstances, the disclosure and processing of those data for the purposes of their subsequent assessment must be based on new circumstances justifying that use (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement  
)   
of 26 July 2017,   
EU:C:2017:592  
, paragraph 200 and the case-law cited).   
219    As to the nature of the circumstances capable of justifying the disclosure and processing of PNR data for the purposes of their subsequent assessment, it is settled case-law that, since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the legislation concerned, be it EU legislation or a national rule intended to transpose the latter, must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of combating crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be inferred that that data might, in a specific case, make an effective contribution to combating such activities (judgments of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 50 and the case-law cited, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 105).  
220    Thus, the terms ‘sufficient grounds’ and ‘reasonably’ in Article 6(2)(b) and Article 12(3)(a), respectively, of the PNR Directive must be interpreted, in the light of Articles 7 and 8 of the Charter, as referring to objective evidence capable of giving rise to a reasonable suspicion that the person concerned is involved in one way or another in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air, whereas, as regards terrorist offences having such a link, that requirement is satisfied when there is objective evidence from which it can be inferred that the PNR data could, in a given case, contribute effectively to combating such offences.   
221    Lastly, as regards the procedural conditions governing the disclosure and processing of PNR data for the purposes of their subsequent assessment, Article 12(3)(b) of the PNR Directive requires, where the request is introduced more than six months after their transfer to the PIU, that is to say when, pursuant to paragraph 2 of that article, those data have been depersonalised through masking out of the elements referred to in that paragraph 2, that the disclosure of the full PNR data and, therefore, of a non-depersonalised version thereof, must be approved by a judicial authority or by another national authority competent under national law. In that context, it is for those authorities to examine in full the merits of the request and, in particular, to ascertain whether the evidence in support of that request is likely to substantiate the substantive condition for the existence of ‘reasonabl[e]’ grounds referred to in the preceding paragraph.  
222    It is true that, where a request for the subsequent disclosure and assessment of PNR data is introduced before the expiry of the period of six months after the transfer of those data, Article 6(2)(b) of the PNR Directive does not expressly provide for such a procedural requirement. Nonetheless, the interpretation of the latter provision must take into consideration recital 25 of that directive, from which it is apparent that, by laying down the said procedural requirement, the EU legislature intended ‘to ensure the highest level of data protection’ concerning access to PNR data in a form which permits direct identification of the data subject. Any request for subsequent disclosure and assessment implies such access to those data, irrespective of whether that request is introduced before the expiry of the period of six months after the transfer of the PNR data to the PIU or whether it is introduced after the expiry of that period.  
223    In particular, in order to ensure, in practice, that fundamental rights are fully observed in the system put in place by the PNR Directive and, in particular, the conditions set out in paragraphs 218 and 219 above, it is essential that disclosure of PNR data for the purposes of subsequent assessment be, as a general rule, except in the event of duly justified urgency, subject to a prior review carried out either by a court or by an independent administrative authority, and that the decision of that court or body be made following a reasoned request by the competent authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. In the event of duly justified urgency, the review must take place within a short time (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraph 202 and the case-law cited, and judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 110).  
224    In those circumstances, the requirement for prior review under Article 12(3)(b) of the PNR Directive, for requests for the disclosure of PNR data introduced after the expiry of a period of six months following the transfer of those data to the PIU must also apply,   
mutatis mutandis  
, where the request for disclosure is introduced before the expiry of that period.  
225    Moreover, if Article 12(3)(b) of the PNR Directive does not expressly specify the requirements which the authority responsible for carrying out the prior review must satisfy, it is settled case-law that, in order to ensure that the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter which results from access to personal data is limited to what is strictly necessary, that authority must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that authority must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258,   
   
paragraph 107 and the case-law cited).  
226    For that purpose, such an authority must have a status that enables it to act objectively and impartially when carrying out its duties and must, therefore, be free from any external influence. That requirement of independence means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review, free from any external influence. In particular, in the criminal field, the requirement of independence entails that the said authority, first, should not be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance vis-a-vis the parties to the criminal proceedings (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 108 and the case-law cited).  
227    Accordingly, the provisions of the PNR Directive governing the subsequent disclosure and assessment of PNR data pursuant to Article 6(2)(b) of that directive lend themselves to an interpretation that is consistent with Articles 7 and 8 as well as Article 52(1) of the Charter and comes within the limits of what is strictly necessary.  
228    In the light of all the foregoing, given that an interpretation of the PNR Directive in the light of Articles 7, 8 and 21 as well as Article 52(1) of the Charter ensures that that directive is consistent with those articles of the Charter, the examination of Questions 2 to 4 and Question 6 has revealed nothing capable of affecting the validity of the said directive.  
C.        
Question 5  
229    By its Question 5, the referring court seeks to ascertain whether Article 6 of the PNR Directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which authorises PNR data collected in accordance with that directive to be processed for the purposes of monitoring activities by the intelligence and security services.  
230    It follows from the request for a preliminary ruling that, by that question, the referring court refers specifically to the activities covered by the Sûreté de l’État (State Security Services, Belgium) and the Service général du renseignement et de la sécurité (General intelligence and security services, Belgium), in the context of their respective duties relating to the protection of national security.  
231    In that regard, in order to comply with the principles of legality and proportionality referred to in Article 52(1) of the Charter, the EU legislature provided clear and precise rules governing the purposes of the measures provided for by the PNR Directive which interfere with the fundamental rights guaranteed in Articles 7 and 8 of the Charter.  
232    Article 1(2) of the PNR Directive states expressly that the PNR data collected in accordance with that directive may be processed ‘only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in points (a), (b) and (c) of Article 6(2) [of the said directive]’. The latter provision confirms the principle set out in that Article 1(2), by referring systematically to the concepts of ‘terrorist offence’ and ‘serious crime’.  
233    It is thus clear from the wording of those provisions that the list included therein of the objectives pursued by the processing of PNR data under the PNR Directive is exhaustive.  
234    That interpretation is supported, inter alia, by recital 11 of the PNR Directive, according to which the processing of PNR data should be proportionate to ‘the specific security goals’ pursued by that directive, and by Article 7(4) thereof, according to which the PNR data and the result of processing those data received by the PIU may be further processed ‘only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime’.  
235    Moreover, the exhaustive nature of the purposes set out in Article 1(2) of the PNR Directive means also that PNR data may not be retained in a single database that may be consulted both for those as well as other purposes. Retention of those data in such a database would entail the risk that those data be used for purposes other than those referred to in that Article 1(2).  
236    In the present case, in so far as, according to the referring court, the national legislation at issue in the main proceedings includes, among the purposes for which PNR data is to be processed, monitoring activities within the remit of the intelligence and security services, thus treating that purpose as an integral part of the prevention, detection, investigation and prosecution of terrorist offences and serious crime, that legislation is liable to disregard the exhaustive nature of the list of the objectives pursued by the processing of PNR data under the PNR Directive, which is a matter for the referring court to verify.   
237    Accordingly, the answer to Question 5 is that Article 6 of the PNR Directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which authorises PNR data collected in accordance with that directive to be processed for purposes other than those expressly referred to in Article 1(2) of the said directive.  
D.        
Question 7  
238    By its Question 7, the referring court asks, in essence, whether Article 12(3)(b) of the PNR Directive must be interpreted as precluding national legislation pursuant to which the authority put in place as the PIU is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.  
239    As a preliminary point, it must be noted that the Belgian Government harbours doubts as to whether the Court has jurisdiction to answer that question, as formulated by the referring court, given that the latter court is the only one with jurisdiction to interpret provisions of national law and, in particular, assess the requirements stemming from the Law of 25 December 2016 in the light of Article 12(3)(b) of the PNR Directive.  
240    In that regard, suffice it to note that, by that question, the referring court is seeking the interpretation of a provision of EU law. In addition, if, in proceedings brought on the basis of Article 267 TFEU, the interpretation of provisions of national law is a matter for the courts of the Member States, not for the Court of Justice, and the Court has no jurisdiction to rule on the compatibility of rules of national law with EU law, the Court does have jurisdiction to provide the national court with all the guidance as to the interpretation of EU law necessary to enable that court to determine whether those national rules are compatible with EU law (judgment of 30 April 2020,   
CTT – Correios de Portugal  
, C-661/18, EU:C:2020:335, paragraph 28 and the case-law cited). It follows that the Court has jurisdiction to answer Question 7.  
241    As to the substance, it should be noted that the wording of Article 12(3)(b) of the PNR Directive, which in its points (i) and (ii) refers to ‘a judicial authority’ and ‘another national authority competent under national law to verify whether the conditions for disclosure are met’, respectively, places both authorities on the same footing as is apparent from the use of the conjunction ‘or’ between those points (i) and (ii). It thus follows from that wording that the ‘other’ competent national authority thus referred to is an alternative to the judicial authority and, accordingly, must have a level of independence and impartiality similar to the latter.  
242    That analysis is supported by the objective of the PNR Directive, mentioned in recital 25 thereof, to ensure the highest level of data protection concerning access to the full PNR data, which enable direct identification of the data subject. That same recital specifies, moreover, that that access should be granted only under very strict conditions after the period of six months following the transfer of PNR data to the PIU.   
243    That analysis is also corroborated by the history of the PNR Directive. Whereas the proposal for a directive mentioned in paragraph 155 above, which became the PNR Directive, simply provided that ‘access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit’, the version of Article 12(3)(b) of that directive finally adopted by the EU legislature designates, placing them on the same footing, the judicial authority and ‘another national authority’ competent to verify whether the conditions for disclosure of the full PNR data are met and approve such disclosure.  
244    In addition and, most importantly, according to the settled case-law recalled in paragraphs 223, 225 and 226 above, it is essential that access to retained data by the competent authorities be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. The requirement of independence that the body responsible for carrying out the prior review must satisfy also means that that body must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially, and free from any external influence. In particular, in the criminal field the requirement of independence entails that the authority responsible for that prior review, first, should not be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance vis-a-vis the parties to the criminal proceedings.  
245    As noted by the Advocate General in point 271 of his Opinion, Article 4 of the PNR Directive, in paragraphs 1 and 3 thereof, provides that the PIU established or designated in each Member State is an authority competent for the prevention, detection, investigation and prosecution of terrorist offences and of serious crime, and that its staff members may be agents seconded from the competent authorities referred to in Article 7 of that directive, so that the PIU appears necessarily linked to those authorities. The PIU may also, pursuant to Article 6(2)(b) of the said directive, process PNR data and disclose the results to the said authorities. In the light of the foregoing, the PIU cannot be considered to be a third party in relation to those authorities and, accordingly, to have all the qualities of independence and impartiality required to carry out the prior review mentioned in the preceding paragraph and verify whether the conditions for disclosure of the full PNR data are met, as provided for in Article 12(3)(b) of that directive.   
246    Furthermore, the fact that the latter provision requires, in its point (ii), where disclosure of the full PNR data has been approved by ‘another [competent] national authority’, that the data protection officer of the PIU ‘[is] inform[ed] and [carries out] an   
ex post  
 review’, whereas this is not the case for approval by the judicial authority, is not such as to call that assessment into question. In accordance with well-established case-law, a subsequent review, such as that carried out by the data protection officer, does not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 110 and the case-law cited).  
247    In the light of all of those considerations, the answer to Question 7 is that Article 12(3)(b) of the PNR Directive must be interpreted as precluding national legislation pursuant to which the authority put in place as the PIU is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.  
E.        
Question 8  
248    By its Question 8, the referring court asks, in essence, whether Article 12 of the PNR Directive, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, without drawing any distinction based on whether or not the passengers concerned present a risk that relates to terrorist offences or serious crime.  
249    It must be recalled that, under Article 12(1) and (4) of that directive, the PIU of the Member State on the territory of which the flight concerned is landing or departing retains the PNR data provided by the air carriers in a database for a period of five years after their transfer to that unit and deletes such data permanently upon expiry of that period of five years.  
250    As recalled in recital 25 of the PNR Directive, ‘the period during which PNR data are to be retained should be as long as is necessary for and proportionate to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime’.  
251    Consequently, the retention of PNR data pursuant to Article 12(1) of the PNR Directive cannot be justified in the absence of an objective connection between that retention and the objectives pursued by that directive, namely the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.   
252    In that regard, as is apparent from recital 25 of the PNR Directive, a distinction must be drawn between, on the one hand, the initial retention period of six months, referred to in Article 12(2) of that directive, and, on the other hand, the later period referred to in Article 12(3) of the said directive.  
253    The interpretation of Article 12(1) of the PNR Directive must take into account the provisions in paragraphs 2 and 3 of that article, which lay down a set of rules for the retention of and access to PNR data retained after expiry of the initial retention period of six months. As is apparent from recital 25 of that directive, those provisions reflect, on the one hand, the objective of ensuring ‘that the PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations’, which may be carried out already during the initial retention period of six months. On the other hand, according to that recital 25, they seek to ‘avoid disproportionate use’ through masking out of those data and to ‘ensure the highest level of data protection’ by granting access to those data in a form which permits direct identification of the data subject ‘only under very strict and limited conditions after that initial period’, thus having regard to the fact that the longer the period for the retention of PNR data, the more serious the resulting interference.  
254    The distinction between the initial retention period of six months referred to in Article 12(2) of the PNR Directive and the later period referred to in Article 12(3) of that directive applies also to the obligation to comply with the requirement referred to in paragraph 251 above.  
255    Thus, in view of the aims pursued by the PNR Directive and of the needs of the investigation and prosecution of terrorist offences and serious crime, the Court finds that the retention, during the initial period of six months, of the PNR data of all air passengers subject to the system established by that directive, without any indication as to their involvement in terrorist offences or serious crime does not appear, as a matter of principle, to go beyond what is strictly necessary, in so far as it allows the necessary searches to be carried out for the purposes of identifying the persons who were not suspected of involvement in terrorist offences or serious crime.   
256    By contrast, as to the later period, set out in Article 12(3) of the PNR Directive, the retention of the PNR data of all air passengers subject to the system established by that directive, in addition to the fact that, by reason of the significant quantity of data that may be retained continuously, it entails an inherent risk of disproportionate use and abuse (see, by analogy, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18,   
EU:C:2020:791  
, paragraph 119), runs counter to the requirement in recital 25 of the said directive that the period during which those data are to be retained should be as long as is necessary for and proportionate to the objectives pursued, since the EU legislature intended to establish the highest level of protection of PNR data allowing direct identification of the data subjects.  
257    As regards air passengers for whom neither the advance assessment under Article 6(2)(a) of the PNR Directive nor any verification carried out during the period of six months referred to in Article 12(2) of that directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with those passengers’ air travel, there would not appear to be, in such circumstances, any connection – even a merely indirect one – between the PNR data of those passengers and the objective pursued by the said directive which would justify the retention of those data (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement  
)   
of 26 July 2017, EU:C:2017:592, paragraphs 204 and 205).  
258    The continued storage of the PNR data of all air passengers after the initial period of six months is not therefore limited to what is strictly necessary (see, by analogy Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraph 206).  
259    However, in so far as, in specific cases, objective evidence, such as the PNR data of passengers which gave rise to a verified positive match, is identified from which it may be inferred that certain passengers may present a risk that relates to terrorist offences or serious crime, it seems permissible to store their PNR data beyond that initial period (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement  
)  
 of 26 July 2017, EU:C:2017:592, paragraph 207 and the case-law cited).  
260    Identification of that objective evidence is capable of establishing a connection with the objectives pursued by processing under the PNR Directive, with the result that the retention of the PNR data of those passengers is justified during the maximum period permitted by the said directive, namely during five years.  
261    In the present case, in so far as the legislation at issue in the main proceedings appears to prescribe a general retention period of five years for PNR data, applicable indiscriminately to all passengers, including those for whom neither the advance assessment under Article 6(2)(a) of the PNR Directive nor any verification carried out in the initial period of six months nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime, that legislation is liable to infringe Article 12(1) of that directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, unless it may be interpreted in a manner that is consistent with those provisions, which is a matter for the referring court to ascertain.  
262    In the light of the foregoing, the answer to the Question 8 is that Article 12(1) of the PNR Directive, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers, including those for whom neither the advance assessment under Article 6(2)(a) of that directive nor any verification carried out during the period of six months referred to in Article 12(2) of the said directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.  
F.        
Question 9(a)  
263    By its Question 9(a), the referring court raises the question, in essence, of the validity of the API Directive in the light of Article 3(2) TEU and Article 45 of the Charter, based on the premiss that the obligations introduced by that directive apply to intra-EU flights.  
264    As noted by the Advocate General in point 277 of his Opinion and as observed by the Council, the Commission and several governments, that premiss is incorrect.  
265    Article 3(1) of the API Directive provides that Member States are to take the necessary steps to establish an obligation for carriers to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State. Those data are to be communicated, pursuant to Article 6(1) of the said directive, to the authorities responsible for carrying out checks at external borders through which the passenger will enter that territory and are to be processed in accordance with the latter provision.  
266    It is clear from those provisions, read in the light of Article 2(a), (b) and (d) of the API Directive, where the concepts of ‘carrier’, ‘external borders’ and ‘border crossing point’, are defined, respectively, that that directive imposes the obligation, for air carriers, to transmit the data referred to in Article 3(2) thereof, to the authorities responsible for carrying out external border checks only in the case of flights transporting passengers to an authorised crossing point for crossing the Member States’ external borders with third countries and provides that only the data relating to those flights are to be processed.   
267    By contrast, the said directive does not impose any obligation concerning the data of passengers travelling on flights that cross only internal borders between Member States.   
268    It should be added that the PNR Directive, by including among PNR data, as is apparent from recital 9 and Article 8(2) thereof, the data referred to in Article 3(2) of the API Directive collected in accordance with that directive and retained by certain air carriers, and by granting Member States the power to apply the PNR Directive, pursuant to Article 2 thereof, to the intra-EU flights selected by them, altered neither the scope of the provisions of the API Directive nor the limitations stemming from that directive.  
269    In the light of the foregoing, the answer to Question 9(a) is that the API Directive must be interpreted as not applying to intra-EU flights.  
G.        
Question 9(b)  
270    While, by its Question 9(b), the referring court refers to the API Directive, read in conjunction with Article 3(2) TEU and Article 45 of the Charter, it is apparent from the request for a preliminary ruling that that court has doubts as to whether the system for the transfer and processing of passenger data established by the Law of 25 December 2016 is compatible with the free movement of persons and the abolition of internal border control provided for by EU law, in that that system applies not only to transport by air, but also transport by rail, by road or even by sea, departing from or going to Belgium and carried out within the European Union, without crossing external borders with third countries.  
271    As is apparent from paragraphs 265 to 269 above, the API Directive, which does not apply to intra-EU flights and does not impose any obligation to transfer and process the data of passengers travelling by air or by another mode of transport within the European Union, without crossing external borders with third countries, is irrelevant for the purposes of answering that question.  
272    However, and whereas, according to Article 67(2) TFEU, the European Union is to ensure the absence of internal border controls for persons, Article 2 of the PNR Directive, on which the Belgian legislature relied to adopt the Law of 25 December 2016 at issue in the main proceedings, as is apparent from the request for a preliminary ruling, authorises Member States to apply that directive to intra-EU flights.  
273    In those circumstances, in order to provide a useful answer to the referring court, it is appropriate to reformulate Question 9(b) as seeking to clarify, in essence, whether EU law, in particular Article 2 of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter, must be interpreted as precluding national legislation which provides for a system for the transfer, by carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of flights and transport operations carried out by other means within the European Union and departing from, going to or transiting through the Member State which adopted the said legislation.  
274    First of all, Article 45 of the Charter enshrines the free movement of persons, which is, moreover, one of the fundamental freedoms of the internal market (see, to that effect, judgment of 22 June 2021,   
Ordre des barreaux francophones et germanophone and Others (Preventive measures for removal)  
, C-718/19, EU:C:2021:505, paragraph 54).   
275    That article guarantees, in paragraph 1 thereof, the right of every citizen of the European Union to move and reside freely within the territory of the Member States, a right which, according to the Explanations relating to the Charter of Fundamental Rights (OJ 2007 C 303, p. 17), corresponds to that guaranteed in the first subparagraph of Article 20(2) TFEU, under (a), and is to be exercised, under the second subparagraph of Article 20(2) TFEU and Article 52(2) of the Charter, in accordance with the conditions and the limits defined by the Treaties and by the measures adopted thereunder.  
276    Next, Article 3(2) TEU provides that the European Union is to offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect, inter alia, to external border controls and the prevention and combating of crime. Similarly, according to Article 67(2) TFEU, the European Union is to ensure the absence of internal border controls for persons and to frame a common policy on, inter alia, external border control.   
277    In accordance with the Court’s established case-law, national legislation which places certain nationals at a disadvantage simply because they have exercised their freedom to move and to reside in another Member State is a restriction of the freedoms conferred by Article 45(1) of the Charter to every Union citizen (see, to that effect, concerning Article 21(1) TFEU, judgments of 8 June 2017,   
Freitag  
, C-541/15, EU:C:2017:432, paragraph 35 and the case-law cited, and of 19 November 2020,   
ZW  
, C-454/19, EU:C:2020:947, paragraph 30).  
278    National legislation such as that at issue in the main proceedings, which applies the system provided for by the PNR Directive not only to extra-EU flights but also, pursuant to Article 2(1) of that directive, to intra-EU flights as well as, beyond what is envisaged under that provision, to transport by other means within the European Union, results in the systematic and continuous transfer and processing of the PNR data of any passenger travelling by those means within the European Union while exercising his or her freedom of movement.   
279    As noted in paragraphs 98 to 111 above, the transfer and processing of data of passengers of extra-EU and intra-EU flights stemming from the system established by the PNR Directive entail undeniably serious interferences with the fundamental rights of the data subjects enshrined in Articles 7 and 8 of the Charter. The seriousness of those interferences is even greater where the application of that system covers other means of transport within the European Union. Such interferences are, for the same reasons as those set out in those paragraphs, also such as to place at a disadvantage and, therefore, deter from exercising their freedom of movement, within the meaning of Article 45 of the Charter, the nationals of the Member States which adopted such a legislation as well as, generally, Union citizens travelling by those means of transport within the European Union from or to those Member States, with the result that that legislation entails a restriction of that fundamental freedom.  
280    In accordance with settled case-law, an obstacle to the freedom of movement of persons can be justified only where it is based on objective considerations and is proportionate to the legitimate objective of the national provisions. A measure is proportionate if, while appropriate for securing the attainment of the objective pursued, it does not go beyond what is necessary in order to attain that objective (see, to that effect, judgment of 5 June 2018,   
Coman and Others  
, C-673/16, EU:C:2018:385, paragraph 41 and the case-law cited).  
281    It should be added that a national measure that is liable to obstruct the exercise of freedom of movement for persons may be justified only where such a measure is consistent with the fundamental rights guaranteed by the Charter, it being the task of the Court to ensure that those rights are respected (judgment of 14 December 2021,   
Stolichna obshtina, rayon ‘Pancharevo’  
, C-490/20, EU:C:2021:1008, paragraph 58 and the case-law cited).  
282    In particular, in accordance with the case-law recalled in paragraphs 115 and 116 above, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue. In that regard, the possibility of Member States justifying a limitation of the right guaranteed in Article 45(1) of the Charter must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness.  
283    As recalled in paragraph 122 above, the objective of combating terrorist offences and serious crime that the PNR Directive pursues is undoubtedly an objective of general interest of the European Union.  
284    As to the question whether national legislation adopted for the purposes of transposing the PNR Directive that extends the system provided for by that directive to intra-EU flights and other modes of transport within the European Union is appropriate for securing the attainment of the objective pursued, it is apparent from the information in the file before the Court that use of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime and who should be subject to further examination, so that such legislation appears to be appropriate for the purpose of attaining the intended objective of combating terrorist offences and serious crime.  
285    As to whether such legislation is necessary, the exercise by the Member States of the power provided for in Article 2(1) of the PNR Directive, read in the light of Articles 7 and 8 of the Charter, must be limited to what is strictly necessary for securing the attainment of that objective in the light of the requirements mentioned in paragraphs 163 to 174 above.  
286    Those requirements apply, a fortiori, where the system provided for by the PNR Directive is applied to other means of transport within the European Union.  
287    Moreover, as follows from the information in the request for a preliminary ruling, the national legislation at issue in the main proceedings transposes, in a single act, the PNR Directive, the API Directive and, in part, Directive 2010/65. To that end, it provides for the application of the system laid down in the PNR Directive to all intra-EU flights and transport by train, by road or even by sea carried out within the European Union departing from, going to or transiting through Belgium, and applies also to tour operators, while also pursuing objectives other than the fight against terrorist offences and serious crime. Following the said information, it appears that all the data collected in the context of the system established by that national legislation are retained by the PIU in a single database encompassing the PNR data, including the data covered by Article 3(2) of the API Directive, for all the passengers of the transport operations covered by that legislation.   
288    In that regard, in so far as the referring court referred to the objective of improving border controls and combating illegal immigration in its Question 9(b), which is the objective of the API Directive, it should be borne in mind that, as follows from paragraphs 233, 234 and 237 above, the list of objectives pursued by the processing of PNR data under the PNR Directive is an exhaustive list with the result that national legislation authorising the processing of PNR data collected in accordance with that directive, for purposes other than those provided for therein, namely for the purposes of improving border controls and combating illegal immigration, is contrary to Article 6 of the said directive, read in the light of the Charter.  
289    In addition, as is apparent from paragraph 235 above, Member States cannot create a single database containing both the PNR data collected under the PNR Directive and relating to extra-EU and intra-EU flights and the data of passengers of other means of transport as well as the data covered by Article 3(2) of the API Directive, in particular where that database can be consulted not only for the purposes referred to in Article 1(2) of the PNR Directive but for other purposes also.   
290    Lastly and in any event, as noted by the Advocate General in point 281 of his Opinion, Articles 28 to 31 of the Law of 25 December 2016 can only be compatible with EU law, and with Article 67(2) TFEU in particular, if they are interpreted and applied as relating only to the transfer and processing of the API data of passengers crossing Belgium’s external borders with third countries. A measure whereby a Member State would extend the provisions of the API Directive, for the purposes of improving border controls and combating illegal immigration, to intra-EU and, a fortiori, other modes of transport carrying passengers within the European Union departing from, going to or transiting through that Member State, in particular the obligation to provide the data covered by Article 3(1) of that directive, would amount to allowing the competent authorities, when internal borders of the said Member State are crossed, to ensure systematically that those passengers can be authorised to enter its territory or to leave it and would thus have an effect equivalent to the checks carried out at external borders with third countries.  
291    In view of all of those considerations, the answer to Question 9(b) is that EU law, in particular Article 2 of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter, must be interpreted as precluding:  
–        national legislation which, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, establishes a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union and departing from, going to or transiting through that Member State, for the purposes of combating terrorist offences and serious crime. In such a situation, the application of the system established by the PNR Directive must be limited to the transfer and processing of the PNR data of flights and/or transport operations relating, inter alia, to certain routes or travel patterns or to certain airports, stations or seaports for which there are indications that are such as to justify that application. It is for the Member State concerned to select the intra-EU flights and/or the transport operations carried out by other means within the European Union for which there are such indications and to review regularly that application in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of that system to those flights and/or those transport operations continues to be limited to what is strictly necessary, and  
–        national legislation providing for such a system for the transfer and processing of those data for the purposes of improving external border controls and combating illegal immigration.  
H.        
Question 10  
292    By its Question 10, the referring court asks, in essence, whether EU law must be interpreted as meaning that a national court may limit the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by land as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Articles 7, 8 and 45 as well as Article 52(1) of the Charter.  
293    The principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State bodies to give full effect to the various provisions of EU law, and the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States. In the light of that principle, where it is unable to interpret national legislation in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means (judgments of 15 July 1964, Costa, 6/64, EU:C:1964:66, pp. 593 and 594; of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18,   
EU:C:2020:791  
, paragraphs 214 and 215; and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 118).  
294    Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested. The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 119 and the case-law cited).  
295    Unlike a breach of a procedural obligation such as the prior assessment of the impact of a project on the environment, at issue in the case that gave rise to the judgment of 29 July 2019,   
Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen  
 (C-411/17,   
EU:C:2019:622  
, paragraphs 175, 176, 179 and 181), in which the Court accepted the temporary suspension of that ousting effect, a failure to comply with the provisions of the PNR Directive, read in the light of Articles 7, 8 and 45 as well as Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure allowed in that case. Maintaining the effects of national legislation such as the Law of 25 December 2016 would mean that that legislation would continue to impose on air carriers and other carriers as well as tour operators obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data have been transferred, retained and processed as well as restrictions on the freedom movement of those persons going beyond what is necessary (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 122 and the case-law cited).  
296    Therefore, the referring court cannot limit the temporal effects of a declaration of illegality which it is bound to make under national law in respect of the national legislation at issue in the main proceedings (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 123 and the case-law cited).  
297    Lastly, in so far as the referring court raises the question of the impact of a finding of incompatibility, if any, of the Law of 25 December 2016 with the provisions of the PNR Directive, read in the light of the Charter, on the admissibility and use of the evidence and information secured from the data transferred by the carriers and tour operators concerned in the context of criminal proceedings, it suffices to refer to the Court’s case-law on that subject, in particular to the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
 (C-746/18, EU:C:2021:152), from which it follows that that admissibility is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 127).  
298    In the light of the foregoing, the answer to the Question 10 is that EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by road as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Articles 7, 8 and 45 as well as Article 52(1) of the Charter. The admissibility of the evidence thus obtained is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.  
IV.      
Costs  
299    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 2(2)(d) and Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, those of Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC and also those of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, in respect of, on the one hand, data processing operations carried out by private operators and, on the other hand, data processing operations carried out by public authorities covered, solely or in addition, by Directive 2004/82 or Directive 2010/65. By contrast, the said regulation does not apply to the data processing operations envisaged by such legislation which are covered only by Directive 2016/681 and are carried out by the passenger information unit (PIU) or by the authorities competent for the purposes referred to in Article 1(2) of that directive.  
2.        
Given that an interpretation of Directive 2016/681 in the light of Articles 7, 8 and 21 as well as Article 52(1) of the Charter of Fundamental Rights of the European Union ensures that that directive is consistent with those articles of the Charter of Fundamental Rights, the examination of Questions 2 to 4 and Question 6 referred for a preliminary ruling has revealed nothing capable of affecting the validity of the said directive.  
3.        
Article 6 of Directive 2016/681, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation which authorises passenger name records (PNR data) collected in accordance with that directive to be processed for purposes other than those expressly referred to in Article 1(2) of the said directive.  
4.        
Article 12(3)(b) of Directive 2016/681 must be interpreted as precluding national legislation pursuant to which the authority put in place as the passenger information unit (PIU) is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.  
5.        
Article 12(1) of Directive 2016/681, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers, including those for whom neither the advance assessment under Article 6(2)(a) of that directive nor any verification carried out during the period of six months referred to in Article 12(2) of the said directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.  
6.        
Directive 2004/82 must be interpreted as not applying to flights, whether scheduled or non-scheduled, carried out by an air carrier flying from the territory of a Member State and that are planned to land on the territory of one or more of the other Member States, without any stop-overs in the territory of a third country (intra-EU flights).  
7.        
EU law, in particular Article 2 of Directive 2016/681, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter of Fundamental Rights, must be interpreted as precluding:  
–          
national legislation which, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, establishes a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union, departing from, going to or transiting through that Member State, for the purposes of combating terrorist offences and serious crime. In such a situation, the application of the system established by Directive 2016/681 must be limited to the transfer and processing of the PNR data of flights and/or transport operations relating, inter alia, to certain routes or travel patterns or to certain airports, stations or seaports for which there are indications that are such as to justify that application. It is for the Member State concerned to select the intra-EU flights and/or the transport operations carried out by other means within the European Union for which there are such indications and to review regularly that application in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of that system to those flights and/or those transport operations continues to be limited to what is strictly necessary, and  
–          
national legislation providing for such a system for the transfer and processing of those data for the purposes of improving external border controls and combating illegal immigration.  
8.        
EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by road as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of Directive 2016/681, read in the light of Article 3(2) TEU, Article 67(2) TFEU, Articles 7, 8 and 45 as well as Article 52(1) of the Charter of Fundamental Rights. The admissibility of the evidence thus obtained is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

ID: 2d57b848-7279-40fe-9d06-57116fd185fe

of 12 Jan 2023, C-154/21 (  
Österreichische Post  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Transparent information, communication and modalities for the exercise of the rights of the data subject   
   
JUDGMENT OF THE COURT (First Chamber)  
12 January 2023 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 15(1)(c) – Data subject’s right of access to his or her data – Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed – Restrictions)  
In Case C-154/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 18 February 2021, received at the Court on 9 March 2021, in the proceedings  
RW  
v  
Österreichische Post AG,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, L. Bay Larsen, Vice-President of the Court, acting as Judge of the First Chamber, P.G. Xuereb, A. Kumin and I. Ziemele (Rapporteur), Judges,  
Advocate General: G. Pitruzzella,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        RW, by R. Haupt, Rechtsanwalt,  
–        Österreichische Post AG, by R. Marko, Rechtsanwalt,  
–        the Austrian Government, by G. Kunnert, A. Posch and J. Schmoll, acting as Agents,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by M. Russo, avvocato dello Stato,  
–        the Latvian Government, by J. Davidoviča, I. Hūna and K. Pommere, acting as Agents,  
–        the Romanian Government, by L.-E. Baţagoi, E. Gane and A. Wellman, acting as Agents,  
–        the Swedish Government, by H. Eklinder, J. Lundberg, C. Meyer-Seitz, A.M. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson, H. Shev and O. Simonsson, acting as Agents,  
–        the European Commission, by F. Erlbacher and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 9 June 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 15(1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (‘the GDPR’).  
2        The request has been made in proceedings between RW and Österreichische Post AG (‘Österreichische Post’) concerning a request for access to personal data pursuant to Article 15(1)(c) of the GDPR.  
   
Legal context  
3        Recitals 4, 9, 10, 39, 63 and 74 of the GDPR are worded as follows:  
‘(4)      … The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. …  
…  
(9)      The objectives and principles of Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)] remain sound, but it has not prevented fragmentation in the implementation of data protection across the [European] Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. …  
…  
(39)      Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. …  
…  
(63)      A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. … Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. … That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. …  
…  
(74)      The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.’  
4        Article 1 of the GDPR, headed ‘Subject matter and objectives’, provides in paragraph 2:  
‘This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.’  
5        Article 5 of the GDPR, headed ‘Principles relating to processing of personal data’, provides:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
…  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
6        Article 12 of the GDPR, headed ‘Transparent information, communication and modalities for the exercise of the rights of the data subject’, states:  
‘1.      The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.  
2.      The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.  
…  
5.      Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:  
(a)      charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or  
(b)      refuse to act on the request.  
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.  
…’  
7        Article 13 of the GDPR, headed ‘Information to be provided where personal data are collected from the data subject’, provides in paragraph 1:  
‘Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:  
…  
(e)      the recipients or categories of recipients of the personal data, if any;  
…’  
8        Article 14 of the GDPR, headed ‘Information to be provided where personal data have not been obtained from the data subject’, provides in paragraph 1:  
‘Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:  
…  
(e)      the recipients or categories of recipients of the personal data, if any;  
…’  
9        As set out in Article 15 of the GDPR, headed ‘Right of access by the data subject’:  
‘1.      The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:  
(a)      the purposes of the processing;  
(b)      the categories of personal data concerned;  
(c)      the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;  
(d)      where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;  
(e)      the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;  
(f)      the right to lodge a complaint with a supervisory authority;  
(g)      where the personal data are not collected from the data subject, any available information as to their source;  
(h)      the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.  
2.      Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.  
3.      The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.  
4.      The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.’  
10      Article 16 of the GDPR, headed ‘Right to rectification’, provides:  
‘The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.’  
11      As set out in Article 17 of the GDPR, headed ‘Right to erasure (“right to be forgotten”)’:  
‘1.      The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:  
(a)      the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;  
(b)      the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;  
(c)      the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);  
(d)      the personal data have been unlawfully processed;  
(e)      the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;  
(f)      the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).  
2.      Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.  
…’  
12      Article 18 of the GDPR, headed ‘Right to restriction of processing’, provides in paragraph 1:  
‘The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:  
(a)      the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;  
(b)      the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;  
(c)      the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;  
(d)      the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.  
…’  
13      Article 19 of the GDPR is worded as follows:  
‘The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.’  
14      Under Article 21 of the GDPR, headed ‘Right to object’:  
‘1.      The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.  
2.      Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.  
3.      Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.  
4.      At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.  
5.      In the context of the use of information society services, and notwithstanding Directive 2002/58/EC [of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37)], the data subject may exercise his or her right to object by automated means using technical specifications.  
6.      Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.’  
15      Article 79 of the GDPR, headed ‘Right to an effective judicial remedy against a controller or processor’, states in paragraph 1:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’  
16      Article 82 of the GDPR, headed ‘Right to compensation and liability’, provides in paragraph 1:  
‘Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.’  
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
17      On 15 January 2019, RW asked Österreichische Post for access under Article 15 of the GDPR to the personal data concerning him which were being stored or had previously been stored by Österreichische Post and, if the data had been disclosed to third parties, for information as to the identity of the recipients.  
18      In response to that request, Österreichische Post merely stated that it uses data, to the extent permissible by law, in the course of its activities as a publisher of telephone directories and that it offers those personal data to trading partners for marketing purposes. It also referred to a website that set out more information and further data processing purposes. It did not disclose to RW the identity of the specific recipients of the data.  
19      RW brought proceedings against Österreichische Post before the Austrian courts, seeking an order that Österreichische Post provide him with, inter alia, the identity of the recipient(s) of the personal data disclosed.  
20      During the judicial proceedings thus initiated, Österreichische Post informed RW that his personal data had been processed for marketing purposes and forwarded to customers, including advertisers trading via mail order and stationary outlets, IT companies, mailing list providers and associations such as charitable organisations, non-governmental organisations (NGOs) or political parties.  
21      The courts at first instance and on appeal dismissed RW’s action on the ground that Article 15(1)(c) of the GDPR, by referring to ‘recipients or categories of recipient’, gives the controller the option of informing the data subject only of the categories of recipient, without having to identify by name the specific recipients to whom personal data are transferred.  
22      RW brought an appeal on a point of law (  
Revision  
) before the Oberster Gerichtshof (Supreme Court, Austria), the referring court.  
23      That court is uncertain as to the interpretation of Article 15(1)(c) of the GDPR, in so far as it is not clear from the wording of that provision whether it grants the data subject the right of access to information relating to the specific recipients of the disclosed data, or whether the controller has discretion as to how it proposes to respond to a request for access to information about the recipients.  
24      The referring court nevertheless observes that the underlying objective of that provision supports the interpretation that it is the data subject who has the option of requesting information about the categories of recipient or requesting information about the specific recipients of his or her personal data. In the referring court’s view, any contrary interpretation would seriously undermine the effectiveness of the legal remedies available to the data subject for the protection of his or her data. If controllers had the option of informing data subjects of the specific recipients or only of the categories of recipient, the fear would be that, in practice, almost no controller would provide information about specific recipients.  
25      In addition, unlike Article 13(1)(e) and Article 14(1)(e) of the GDPR, which lay down an obligation on the part of the controller to provide the information set out in those articles, Article 15(1) of that regulation focuses on the scope of the data subject’s right of access, a fact which, according to the referring court, also tends to indicate that the data subject has the right to choose between requesting information about the specific recipients or about categories of recipient.  
26      Lastly, the referring court adds that the right of access provided for in Article 15(1) of the GDPR covers not only personal data currently being processed but also all data processed previously. In that regard, it states that the considerations set out in the judgment of 7 May 2009,   
Rijkeboer  
 (C-553/07, EU:C:2009:293), based on the purpose of the right of access provided for by Directive 95/46, may be transferred to the right of access under Article 15 of the GDPR, especially since it can be deduced from recitals 9 and 10 of the GDPR that the EU legislature did not intend to reduce the level of protection as compared to that directive.  
27      In those circumstances, the Oberster Gerichtshof (Supreme Court) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
‘Is Article 15(1)(c) of [the GDPR] to be interpreted as meaning that the right of access is limited to information concerning categories of recipient where specific recipients have not yet been determined in the case of planned disclosures, but that right must necessarily also cover recipients of those disclosures in cases where data [have] already been disclosed?’  
   
Consideration of the question referred  
28      By its question, the referring court asks, in essence, whether Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject’s right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the specific identity of those recipients.  
29      As a preliminary point, it should be borne in mind that, in accordance with settled case-law, the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 15 March 2022,   
Autorité des marchés financiers  
, C-302/20, EU:C:2022:190, paragraph 63). Furthermore, where a provision of EU law is open to several interpretations, preference must be given to that interpretation which ensures that the provision retains its effectiveness (judgment of 7 March 2018,   
Cristal Union  
, C-31/17, EU:C:2018:168, paragraph 41 and the case-law cited).  
30      As regards, first of all, the wording of Article 15(1)(c) of the GDPR, that provision states that the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and information about the recipients or categories of recipient to whom the personal data have been or will be disclosed.  
31      It should be noted that the terms ‘recipients’ and ‘categories of recipient’ in that provision are used in succession, without it being possible to infer an order of priority between them.  
32      It is thus clear that the wording of Article 15(1)(c) of the GDPR does not make it possible to determine unequivocally whether the data subject would have the right to be informed, when personal data concerning him or her have been or will be disclosed, of the specific identity of the recipients of the data.  
33      Next, as regards the context of Article 15(1)(c) of the GDPR, it should be pointed out, in the first place, that recital 63 of that regulation states that the data subject is to have the right to know and obtain communication in particular with regard to the recipients of the personal data and does not state that that right may be restricted solely to categories of recipient, as the Advocate General observed in point 23 of his Opinion.  
34      In the second place, it should also be borne in mind that, in order to respect the right of access, all processing of personal data of natural persons must comply with the principles set out in Article 5 of the GDPR (see, to that effect, judgment of 16 January 2019,   
Deutsche Post  
, C-496/17, EU:C:2019:26, paragraph 57).  
35      Those principles include the principle of transparency set out in Article 5(1)(a) of the GDPR, which, as is clear from recital 39 of that regulation, requires that the data subject have information about how his or her personal data are processed and that that information be easily accessible and easy to understand.  
36      In the third place, it should be noted, as the Advocate General stated in point 21 of his Opinion, that, unlike Articles 13 and 14 of the GDPR, which lay down an obligation on the part of the controller to provide the data subject with information relating to the categories of recipient or the specific recipients of the personal data concerning him or her where personal data are collected from the data subject and where personal data have not been obtained from the data subject, Article 15 of the GDPR lays down a genuine right of access for the data subject, with the result that the data subject must have the option of obtaining either information about the specific recipients to whom the data have been or will be disclosed, where possible, or information about the categories of recipient.  
37      In the fourth place, the Court has previously held that the exercise of that right of access must enable the data subject to verify not only that the data concerning him or her are correct, but also that they are processed in a lawful manner (see, by analogy, judgments of 17 July 2014,   
YS and Others  
, C-141/12 and C-372/12, EU:C:2014:2081, paragraph 44, and of 20 December 2017,   
Nowak  
, C-434/16, EU:C:2017:994, paragraph 57), and in particular that they have been disclosed to authorised recipients (see, by analogy, judgment of 7 May 2009,   
Rijkeboer  
, C-553/07, EU:C:2009:293, paragraph 49).  
38      In particular, that right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her right to rectification, right to erasure (‘right to be forgotten’) or right to restriction of processing, conferred, respectively, by Articles 16, 17 and 18 of the GDPR (see, by analogy, judgments of 17 July 2014,   
YS and Others  
, C-141/12 and C-372/12, EU:C:2014:2081, paragraph 44, and of 20 December 2017,   
Nowak  
, C-434/16, EU:C:2017:994, paragraph 57), and the data subject’s right to object to his or her personal data being processed, laid down in Article 21 of the GDPR, and right of action where he or she suffers damage, laid down in Articles 79 and 82 of the GDPR (see, by analogy, judgment of 7 May 2009,   
Rijkeboer  
, C-553/07, EU:C:2009:293, paragraph 52).  
39      Thus, in order to ensure the effectiveness of all of the rights referred to in the preceding paragraph of the present judgment, the data subject must have, in particular, the right to be informed of the identity of the specific recipients where his or her personal data have already been disclosed.  
40      Such an interpretation is confirmed, in the fifth and last place, by a reading of Article 19 of the GDPR, which provides, in its first sentence, that the controller is, in principle, to communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed and, in its second sentence, that the controller is to inform the data subject about those recipients if the data subject requests it.  
41      Thus, the second sentence of Article 19 of the GDPR expressly confers on the data subject the right to be informed of the specific recipients of the data concerning him or her by the controller, in the context of the controller’s obligation to inform all the recipients of the exercise of the data subject’s rights under Article 16, Article 17(1) and Article 18 of the GDPR.  
42      It follows from the above contextual analysis that Article 15(1)(c) of the GDPR is one of the provisions intended to ensure transparency vis-à-vis the data subject of the manner in which personal data are processed and enables that person, as the Advocate General observed in point 33 of his Opinion, to exercise the rights laid down, inter alia, in Articles 16 to 19, 21, 79 and 82 of the GDPR.  
43      Accordingly, the information provided to the data subject pursuant to the right of access provided for in Article 15(1)(c) of the GDPR must be as precise as possible. In particular, that right of access entails the ability of the data subject to obtain from the controller information about the specific recipients to whom the data have been or will be disclosed or, alternatively, to elect merely to request information concerning the categories of recipient.  
44      Lastly, as regards the purpose of the GDPR, it should be pointed out that its purpose is, inter alia, as is apparent from recital 10 of that regulation, to ensure a high level of protection of natural persons within the European Union (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 207). In that regard, as the Advocate General observed, in essence, in point 14 of his Opinion, the general legal framework created by the GDPR implements the requirements arising from the fundamental right, protected by Article 8 of the Charter of Fundamental Rights of the European Union, to the protection of personal data, in particular the requirements expressly laid down in Article 8(2) thereof (see, to that effect, judgment of 9 March 2017,   
Manni  
, C-398/15, EU:C:2017:197, paragraph 40).  
45      That objective supports the interpretation of Article 15(1) of the GDPR set out in paragraph 43 above.  
46      Therefore, it also follows from the objective pursued by the GDPR that the data subject has the right to obtain from the controller information about the specific recipients to whom the personal data concerning him or her have been or will be disclosed.  
47      That said, it must, lastly, be emphasised that, as is apparent from recital 4 of the GDPR, the right to the protection of personal data is not an absolute right. That right must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality, as the Court reaffirmed, in essence, in paragraph 172 of the judgment of 16 July 2020,   
Facebook Ireland and Schrems  
 (C-311/18, EU:C:2020:559).  
48      Accordingly, it may be accepted that, in specific circumstances, it is not possible to provide information about specific recipients. Therefore, the right of access may be restricted to information about categories of recipient if it is impossible to disclose the identity of specific recipients, in particular where they are not yet known.  
49      In addition, it should be borne in mind that, under Article 12(5)(b) of the GDPR, the controller may, pursuant to the principle of responsibility referred to in Article 5(2) and recital 74 of that regulation, refuse to act on requests from a data subject where those requests are manifestly unfounded or excessive, it being specified that it is for the controller to demonstrate that those requests are unfounded or excessive.  
50      In the present case, it is apparent from the request for a preliminary ruling that Österreichische Post refused the request made by RW under Article 15(1) of the GDPR to be informed of the identity of the recipients to whom Österreichische Post had disclosed the personal data concerning him. It will be for the referring court to determine whether, in the light of the circumstances of the main proceedings, Österreichische Post has demonstrated that that request is manifestly unfounded or excessive.  
51      In the light of all the foregoing considerations, the answer to the question referred for a preliminary ruling is that Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject’s right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the actual identity of those recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject’s requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of the GDPR, in which cases the controller may indicate to the data subject only the categories of recipient in question.  
   
Costs  
52      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
Article 15(1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),  
must be interpreted as meaning that the data subject’s right of access to the personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the actual identity of those recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject’s requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of Regulation 2016/679, in which cases the controller may indicate to the data subject only the categories of recipient in question.

ID: 316faec1-57a5-4756-aabc-346c99097ef8

Judgment of 19 Apr 2012, C-461/10 (  
Bonnier Audio and Others  
)  
Data Retention Directive   
E-privacy Directive   
 >   
Electronic communications   
 >   
Data retention and access of national authorities   
   
JUDGMENT OF THE COURT (Third Chamber)  
19 April 2012 (\*)  
(Copyright and related rights — Processing of data by internet — Infringement of an exclusive right — Audio books made available via an FTP server via internet by an IP address supplied by an internet service provider — Injunction issued against the internet service provider ordering it to provide the name and address of the user of the IP address)  
In Case C-461/10,  
REFERENCE for a preliminary ruling under Article 267 TFEU from the Högsta domstolen (Sweden), made by decision of 25 August 2010, received at the Court on 20 September 2010, in the proceedings  
Bonnier Audio AB,  
Earbooks AB,  
Norstedts Förlagsgrupp AB,  
Piratförlaget AB,  
Storyside AB  
v  
Perfect Communication Sweden AB,  
THE COURT (Third Chamber),  
composed of K. Lenaerts, President of the Chamber, J. Malenovský, (Rapporteur), R. Silva de Lapuerta, E. Juhász and D. Šváby, Judges,  
Advocate General: N. Jääskinen,  
Registrar: K. Sztranc-Sławiczek, Administrator,  
having regard to the written procedure and further to the hearing on 30 June 2011,  
after considering the observations submitted on behalf of:  
–        Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB and Storyside AB, by P. Danowsky and O. Roos, advokater,  
–        Perfect Communication Sweden AB, by P. Helle and M. Moström, advokater,  
–        the Swedish Government, by A. Falk and C. Meyer-Seitz, acting as Agents,  
–        the Czech Government, by M. Smolek and K. Havlíčková, acting as Agents,  
–        the Italian Government, by G. Palmieri and C. Colelli, acting as Agents, and by S. Fiorentino, avvocato dello Stato,  
–        the Latvian Government, by M. Borkoveca and K. Krasovska, acting as Agents,  
–        the European Commission, by R. Troosters and K. Simonsson, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 17 November 2011,  
gives the following  
Judgment  
1        This reference for a preliminary ruling concerns the interpretation of Articles 3 to 5 and 11 of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), and of Article 8 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum OJ 2004 L 195, p. 16).   
2        The reference has been made in proceedings between (i) Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB and Storyside AB (‘the applicants in the main proceedings’) and (ii) Perfect Communications Sweden AB (‘ePhone’) concerning the latter’s opposition to an injunction obtained by the applicants in the main proceedings ordering the disclosure of data.   
   
Legal context   
   
European Union law  
 Provisions concerning the protection of intellectual property   
3        Article 8 of Directive 2004/48 reads as follows:  
‘1.      Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:  
(a)      was found in possession of the infringing goods on a commercial scale;  
(b)      was found to be using the infringing services on a commercial scale;  
(c)      was found to be providing on a commercial scale services used in infringing activities;  
or  
(d)      was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.  
2.      The information referred to in paragraph 1 shall, as appropriate, comprise:  
(a)      the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;  
(b)      information on the quantities produced, manufactured, delivered, received or ordered, as well as the price obtained for the goods or services in question.  
3.      Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which:  
(a)      grant the rightholder rights to receive fuller information;  
(b)      govern the use in civil or criminal proceedings of the information communicated pursuant to this article;  
(c)      govern responsibility for misuse of the right of information;  
or  
(d)      afford an opportunity for refusing to provide information which would force the person referred to in paragraph 1 to admit to his/her own participation or that of his/her close relatives in an infringement of an intellectual property right;   
or   
(e)      govern the protection of confidentiality of information sources or the processing of personal data.’   
 Provisions concerning the protection of personal data  
–       Directive 95/46/EC  
4        Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) lays down rules relating to the processing of personal data in order to protect the rights of individuals in that respect, while ensuring the free movement of those data in the European Union.  
5        Article 2(a) and (b) of Directive 95/46 states:  
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.’   
6        Article 13 of that directive, entitled ‘Exemptions and restrictions’, provides in paragraph 1:  
‘Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:   
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
(e)      an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;  
(f)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);  
(g)      the protection of the data subject or of the rights and freedoms of others.’  
–       Directive 2002/58/EC  
7        Under Article 2 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37):   
‘Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ L 108, p. 33)] shall apply.  
The following definitions shall also apply:  
…  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;   
…  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;   
…’  
8        Article 5(1) of Directive 2002/58 provides:  
‘Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.’   
9        Article 6 of Directive 2002/58 provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this article and Article 15(1).   
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.   
6.      Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.’   
10      Under Article 15(1) of that directive:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’   
–       Directive 2006/24  
11      In accordance with recital 12 in the preamble to Directive 2006/24:  
‘Article 15(1) of Directive 2002/58/EC continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive.’   
12      Article 1(1) of Directive 2006/24 states:  
‘This Directive aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.’   
13      Article 3(1) of that directive provides:  
‘By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.’   
14      Article 4 of that directive states:  
‘Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the [European Convention on Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950,] as interpreted by the European Court of Human Rights.’  
15      Article 5 of Directive 2006/24 states:  
‘1.      Member States shall ensure that the following categories of data are retained under this Directive:  
(a)      data necessary to trace and identify the source of a communication:  
(1)      concerning fixed network telephony and mobile telephony:  
(i)      the calling telephone number;  
(ii)      the name and address of the subscriber or registered user;  
(2)      concerning Internet access, Internet e-mail and Internet telephony:  
(i)      the user ID(s) allocated;  
(ii)      the user ID and telephone number allocated to any communication entering the public telephone network;  
(iii)       the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;  
(b)      data necessary to identify the destination of a communication:  
…  
(c)      data necessary to identify the date, time and duration of a communication:  
…  
(d)      data necessary to identify the type of communication:  
…  
(e)      data necessary to identify users’ communication equipment or what purports to be their equipment:  
…  
(f)      data necessary to identify the location of mobile communication equipment:  
…  
2.      No data revealing the content of the communication may be retained pursuant to this Directive.’   
16      Article 6 of that directive, concerning the periods of retention, provides:  
‘Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.’  
17      Article 11 of that directive reads as follows:  
‘The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:  
“1a. Paragraph 1 shall not apply to data specifically required by [Directive 2006/24] to be retained for the purposes referred to in Article 1(1) of that Directive.”’  
   
National law  
 Copyright  
18      The provisions of Directive 2004/48 were transposed into Swedish law by the insertion of new provisions into Law 1960:729 on copyright in literary and artistic works (lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk) by Law (2009:109) amending Law 1960:729 (lagen (2009:109) om ändring i lagen (1960:729)) of 26 February 2009 (‘the Law on copyright’). Those new provisions entered into force on 1 April 2009.   
19      Paragraph 53c of the Law on copyright provides:  
‘If the applicant shows clear evidence that someone has committed an infringement referred to in Paragraph 53, the court may order one or more of the persons referred to in the second paragraph below, on penalty of a fine, to provide the applicant with information on the origin and distribution network of the goods or services affected by the infringement (order for disclosure of information). Such an order may be made at the request of an author or a successor in title of an author or a person who, on the basis of a licence, is entitled to exploit the work. It may be made only if the information can be regarded as facilitating the investigation into an infringement concerning the goods or services.  
The obligation to disclose information applies to any person who  
(1)      has carried out or contributed to the infringement,   
(2)      has, on a commercial scale, exploited the goods affected by the infringement,  
(3)      has, on a commercial scale, exploited a service affected by the infringement,   
(4)      has, on a commercial scale, provided an electronic communications service or another service used in the infringement, or  
(5)      has been identified by a person referred to in points (2) to (4) as participating in the production or distribution of goods or the supply of services affected by the infringement.  
Information on the origin or distribution network of goods or services may include, inter alia  
(1)      the name and address of producers, distributors, suppliers and others who have held the goods or supplied the services,  
(2)      the names and addresses of intended wholesalers and retailers, and  
(3)      information concerning the quantities produced, supplied, received or ordered and the price fixed for the goods or services.   
The provisions in the first to third subparagraphs above also apply to attempts or preparations made to commit infringements referred to in Paragraph 53.’   
20      Paragraph 53d of that Law provides:  
‘An order for disclosure of information may be made only if the reasons for the measure outweigh the nuisance or other harm which the measure entails for the person affected by it or for some other conflicting interest.   
The obligation to disclose information under Paragraph 53c does not cover information disclosure of which would reveal that the person disclosing that information or persons close to him within the meaning of Chapter 36, Paragraph 3, of the Code of Judicial Procedure (rättegångsbalken) has committed a criminal act.   
There are provisions in the Law (1998:204) on personal data (personuppgiftslagen (1998:204)) which restrict the manner in which personal data received may be handled.’   
 Protection of personal data   
21      Directive 2002/58 was transposed into Swedish law in particular by Law (2003:389) on electronic communications (lagen (2003:389) om elektronisk kommunikation).  
22      Under the first sentence of Paragraph 20 of that Law, a person who, in connection with the provision of an electronic communications network or an electronic communications service, has acquired or been given access to, inter alia, data on subscriptions may not without authorisation disseminate or exploit the data which he has acquired or to which he has been given access.  
23      The national court notes in that regard that the obligation of confidentiality to which internet service providers in particular are subject has been conceived to prohibit only unauthorised disclosure or use of certain data. However, that obligation of confidentiality is relative, since other provisions require that information to be disclosed, which means that such disclosure is not unauthorised. According to the Högsta domstolen, the right to information provided for in Paragraph 53c of the Law on copyright, which also applies to internet service providers, was deemed not to require the implementation of specific legislative changes in order to enable the new provisions relating to disclosure of personal data to take precedence over the obligation of confidentiality. The obligation of confidentiality is therefore overridden by the court’s decision on an order for disclosure of information.   
24      Directive 2006/24 has not been transposed into Swedish law within the time-limit prescribed.   
   
The dispute in the main proceedings and the questions referred for a preliminary ruling   
25      The applicants in the main proceedings are publishing companies which hold, inter alia, exclusive rights to the reproduction, publishing and distribution to the public of 27 works in the form of audio books.  
26      They claim that their exclusive rights have been infringed by the public distribution of these 27 works, without their consent, by means of an FTP (‘file transfer protocol’) server which allows file sharing and data transfer between computers connected to the internet.  
27      The internet service provider through which the alleged illegal file exchange took place is ePhone.  
28      The applicants in the main proceedings applied to Solna tingsrätten (Solna District Court) for an order for the disclosure of data for the purpose of communicating the name and address of the person using the IP address from which it is assumed that the files in question were sent during the period between 03:28 and 05:45 on 1 April 2009.  
29      The service provider, ePhone, challenged this application, arguing in particular that the injunction sought is contrary to Directive 2006/24.  
30      At first instance, Solna tingsrätten granted the application for an order for the disclosure of the data in question.  
31      ePhone brought an appeal before Svea hovrätten (Stockholm Court of Appeal), seeking dismissal of the application for the order for the disclosure. It also requested a referral to the Court of Justice seeking clarification of whether Directive 2006/24 precludes the disclosure to persons other than the authorities referred to in the directive of information relating to a subscriber to whom an IP address has been allocated.  
32      Svea hovrätten held that there is no provision in Directive 2006/24 which precludes a party to a civil dispute from being ordered to disclose subscriber data to someone other than a public authority. It also dismissed the application for a referral to the Court of Justice.   
33      Svea hovrätten also found that the audio book publishers had not adduced clear evidence that there was an infringement of an intellectual property right. It therefore decided to set aside the order for disclosure of data granted by Solna tingsrätten. The applicants in the main proceedings then appealed to the Högsta domstolen.  
34      The Högsta domstolen is of the opinion that, notwithstanding the judgment in Case C-275/06   
Promusicae   
[2008] ECR I-271 and the order in Case C-557/07   
LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten  
 [2009] ECR I-1227, doubts remain as to whether European Union law precludes the application of Article 53c of the Swedish Law on copyright, in so far as neither that judgment nor that order makes reference to Directive 2006/24.   
35      In those circumstances, the Högsta domstolen decided to stay the proceedings and refer to the following questions to the Court for a preliminary ruling:  
‘1.      Does [Directive 2006/24], and in particular Articles 3 [to] 5 and 11 thereof, preclude the application of a national provision which is based on Article 8 of [Directive 2004/48] and which permits an internet service provider in civil proceedings, in order to identify a particular subscriber, to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided a specific IP address, which address, it is claimed, was used in the infringement? The question is based on the assumption that the applicant has adduced clear evidence of the infringement of a particular copyright and that the measure is proportionate.  
2.      Is the answer to Question 1 affected by the fact that the Member State has not implemented [Directive 2006/24] despite the fact that the period prescribed for implementation has expired?’   
   
Consideration of the questions referred   
36      By its two questions, which it is appropriate to consider together, the national court asks, in essence, whether Directive 2006/24 is to be interpreted as precluding the application of a national provision based on Article 8 of [Directive 2004/48] which, in order to identify a particular subscriber, permits an internet service provider in civil proceedings to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in the infringement, and whether the fact that the Member State concerned has not yet transposed Directive 2006/24, despite the period for doing so having expired, affects the answer to that question.  
37      As a preliminary point, it must be noted, firstly, that the Court is starting from the premiss that the data at issue in the main proceedings have been retained in accordance with national legislation, in compliance with the conditions laid down in Article 15(1) of Directive 2002/58, a matter which it is for the national court to ascertain.  
38      Secondly, Directive 2006/24, according to Article 1(1) thereof, aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.   
39      Furthermore, as follows from Article 4 of Directive 2006/24, the data retained in accordance with that directive are to be provided only to the competent national authorities in specific cases and in accordance with the national law concerned.  
40      Thus, Directive 2006/24 deals exclusively with the handling and retention of data generated or processed by the providers of publicly available electronic communications services or public communications networks for the purpose of the investigation, detection and prosecution of serious crime and their communication to the competent national authorities.   
41      The material scope of Directive 2006/24 thus stated is confirmed by Article 11 thereof which states that, if such data were retained specifically for the purposes of Article 1(1) of the directive, Article 15(1) of Directive 2002/58 does not apply to those data.  
42      However, as is apparent from recital 12 in the preamble to Directive 2006/24, Article 15(1) of Directive 2002/58/EC continues to apply to data retained for purposes, including judicial purposes, other than those referred to expressly in Article 1(1) of Directive 2006/24.   
43      Thus, it follows from a combined reading of Article 11 and recital 12 of Directive 2006/24 that that directive constitutes a special and restricted set of rules, derogating from and replacing Directive 2002/58 general in scope and, in particular, Article 15(1) thereof.  
44      With regard to the main proceedings, it must be noted that the legislation at issue pursues an objective different from that pursued by Directive 2006/24. It concerns the communication of data, in civil proceedings, in order to obtain a declaration that there has been an infringement of intellectual property rights.   
45      That legislation does not, therefore, fall within the material scope of Directive 2006/24.  
46      Accordingly, it is irrelevant to the main proceedings that the Member State concerned has not yet transposed Directive 2006/24, despite the period for doing so having expired.   
47      None the less, in order to provide a satisfactory answer to the national court which has referred a question to it, the Court of Justice may also deem it necessary to consider provisions of European Union law to which the national court has not referred in its question (see, inter alia, Case C-107/98   
Teckal  
 [1999] ECR I-8121, paragraph 39, and Case C-2/07   
Abraham and Others  
 [2008] ECR I-1197, paragraph 24).  
48      It must be noted that the facts in the main proceedings lend themselves to such rules of European Union law being taken into consideration.   
49      The reference made by the national court, in its first question, to compliance with the requirement for clear evidence of an infringement of a copyright and to the proportionate nature of the injunction which would be issued under the transposing law at issue in the main proceedings and, as follows from paragraph 34 of the present judgment, to the judgment in   
Promusicae  
, suggests that the national court is also doubtful as to whether the provisions in question of that transposing law are likely to ensure a fair balance between the various applicable fundamental rights, as required by that judgment, which interpreted and applied various provisions of Directives 2002/58 and 2004/48.  
50      Thus, the answer to such an implied question may be relevant to the resolution of the case in the main proceedings.  
51      In order to give a useful answer, firstly, it is necessary to bear in mind that the applicants in the main proceedings seek the communication of the name and address of an internet subscriber or user using the IP address from which it is presumed that an unlawful exchange of files containing protected works took place, in order to identify that person.  
52      It must be held that the communication sought by the applicants in the main proceedings constitutes the processing of personal data within the meaning of the first paragraph of Article 2 of Directive 2002/58, read in conjunction with Article 2(b) of Directive 95/46. That communication therefore falls within the scope of Directive 2002/58 (see, to that effect,   
Promusicae  
, paragraph 45).   
53      It must also be noted that, in the main proceedings, the communication of those data is required in civil proceedings for the benefit of a copyright holder or his successor in title, that is to say, a private person, and not for the benefit of a competent national authority.  
54      In that regard, it must be stated at the outset that an application for communication of personal data in order to ensure effective protection of copyright falls, by its very object, within the scope of Directive 2004/48 (see, to that effect,   
Promusicae  
, paragraph 58).   
55      The Court has already held that Article 8(3) of Directive 2004/48, read in conjunction with Article 15(1) of Directive 2002/58, does not preclude Member States from imposing an obligation to disclose to private persons personal data in order to enable them to bring civil proceedings for copyright infringements, but nor does it require those Member States to lay down such an obligation (see   
Promusicae  
, paragraphs 54 and 55, and order in   
LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten  
, paragraph 29).   
56      However, the Court pointed out that, when transposing, inter alia, Directives 2002/58 and 2004/48 into national law, it is for the Member States to ensure that they rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights protected by the European Union legal order. Furthermore, when implementing the measures transposing those directives, the authorities and courts of Member States must not only interpret their national law in a manner consistent with them, but must also make sure that they do not rely on an interpretation of them which would conflict with those fundamental rights or with the other general principles of European Union law, such as the principle of proportionality (see, to that effect,   
Promusicae  
, paragraph 68, and order in   
LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten  
, paragraph 28).  
57      In the present case, the Member State concerned has decided to make use of the possibility available to it, as described in paragraph 55 of this judgment, to lay down an obligation to communicate personal data to private persons in civil proceedings.  
58      It must be noted that the national legislation in question requires, inter alia, that, for an order for disclosure of the data in question to be made, there be clear evidence of an infringement of an intellectual property right, that the information can be regarded as facilitating the investigation into an infringement of copyright or impairment of such a right and that the reasons for the measure outweigh the nuisance or other harm which the measure may entail for the person affected by it or for some other conflicting interest.  
59      Thus, that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality.  
60      In those circumstances, such legislation must be regarded as likely, in principle, to ensure a fair balance between the protection of intellectual property rights enjoyed by copyright holders and the protection of personal data enjoyed by internet subscribers or users.  
61      Having regard to the foregoing, the answer to the questions referred is that:  
–        Directive 2006/24 must be interpreted as not precluding the application of national legislation based on Article 8 of Directive 2004/48 which, in order to identify an internet subscriber or user, permits an internet service provider in civil proceedings to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in an infringement, since that legislation does not fall within the material scope of Directive 2006/24;  
–        it is irrelevant to the main proceedings that the Member State concerned has not yet transposed Directive 2006/24, despite the period for doing so having expired;  
–        Directives 2002/58 and 2004/48 must be interpreted as not precluding national legislation such as that at issue in the main proceedings insofar as that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality.  
   
Costs  
62      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC must be interpreted as not precluding the application of national legislation based on Article 8 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights which, in order to identify an internet subscriber or user, permits an internet service provider in civil proceedings to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in an infringement, since that legislation does not fall within the material scope of Directive 2006/24.  
It is irrelevant to the main proceedings that the Member State concerned has not yet transposed Directive 2006/24, despite the period for doing so having expired.  
Directives 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and 2004/48 must be interpreted as not precluding national legislation such as that at issue in the main proceedings insofar as that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality.

ID: 34015f7b-149d-4f22-8fcb-9ad4dc0868d2

Judgment of 10 Jul 2018, C-25/17 (  
Jehovan todistajat  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Household exemption   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Filing System   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Joint controllers   
   
JUDGMENT OF THE COURT (Grand Chamber)  
10 July 2018 (\*)  
(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Scope of the directive — Article 3 — Data collected and processed by the members of a religious community in the course of their door-to-door preaching — Article 2(c) — Definition of a ‘personal data filing system’ — Article 2(d) — Definition of a ‘controller’ of the processing of personal data — Article 10(1) of the Charter of Fundamental Rights of the European Union)  
In Case C-25/17,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Korkein hallinto-oikeus (Supreme Administrative Court, Finland), made by decision of 22 December 2016, received at the Court on 19 January 2017, in the proceedings  
Tietosuojavaltuutettu  
intervening parties:  
Jehovan todistajat — uskonnollinen yhdyskunta,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Tizzano, Vice-President, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), J.L. da Cruz Vilaça, J. Malenovský, E. Levits and C. Vajda, Presidents of Chambers, A. Borg Barthet, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen, K. Jürimäe and C. Lycourgos, Judges,  
Advocate General: P. Mengozzi,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 28 November 2017,  
after considering the observations submitted on behalf of:  
–        the tietosuojavaltuutettu, by R. Aarnio, acting as Agent,  
–        Jehovan todistajat — uskonnollinen yhdyskunta, by S.H. Brady, asianajaja, and by P. Muzny,  
–        the Finnish Government, by H. Leppo, acting as Agent,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by P. Gentili, avvocato dello Stato,  
–        the European Commission, by P. Aalto, H. Kranenborg and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 1 February 2018,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2(c) and (d) and Article 3 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) read in the light of Article 10 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings brought by the tietosuojavaltuutettu (Data Protection Supervisor, Finland) concerning the legality of a decision of the tietosuojalautakunta (Data Protection Board, Finland) prohibiting the Jehovan todistajat — uskonnollinen yhdyskunta (Jehovah’s Witnesses religious community, ‘the Jehovah’s Witnesses Community’) from collecting or processing personal data in the course of their door-to-door preaching unless the requirements of Finnish legislation relating to the processing of personal data are observed.  
   
Legal context  
   
European Union law  
3        Recitals 10, 12, 15, 26 and 27 of Directive 95/46 state:  
‘(10)      Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;  
…  
(12)      Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;  
…  
(15)      Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;  
…  
(26)      Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; …  
(27)      Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2(c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive’.  
4        Article 1(1) of Directive 95/46 provides:  
‘In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.’  
5        Article 2 of that directive provides:  
‘For the purpose of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
(c)      “personal data filing system” (“filing system”) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;  
…’  
6        Article 3 of the directive states:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
   
Finnish law  
7        Directive 95/46 was transposed into Finnish law by the henkilötietolaki 523/1999 (Law on personal data No 523/1999, ‘Law No 523/1999’).  
8        Paragraph 2, first and second paragraphs, of that law, entitled ‘Soveltamisala’ (Scope), provides;  
‘This Law applies to the automated processing of personal data. It also applies to other means of personal data processing where the personal data form part of a personal data filing system or a part of such a system or are intended to form part of a personal data filing system or a part of such a system.  
This Law does not apply to the processing of personal data by a natural person for purely personal purposes or for comparable ordinary and private purposes.’  
9        Paragraph 3(3) of Law No 523/1999 defines a ‘personal data filing system’ as a ‘set of personal data, connected by a common use and processed fully or partially by automated means or organised using data sheets or lists or any other comparable means permitting the retrieval of data relating to persons easily and without excessive cost’.  
10      In accordance with Paragraph 44 of that law, at the request of the Data Protection Supervisor, the Data Protection Board may prohibit processing of personal data that is contrary to that law or to the rules and regulations issued on the basis thereof, and order the parties concerned to remedy the unlawful conduct or negligence within a prescribed period.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
11      On 17 September 2013, at the request of the Data Protection Supervisor the Finnish Data Protection Board adopted a decision prohibiting the Jehovah’s Witnesses Community from collecting or processing personal data in the course of door-to-door preaching carried out by its members unless the legal requirements for processing such data laid down, in particular, in Paragraphs 8 and 12 of the Law No 523/1999 were satisfied. Furthermore, on the basis of Paragraph 44(2) of that law, the Data Protection Board imposed a ban on the collection of personal data by the Jehovah’s Witnesses Community for the purposes of that community for a period of six months unless those conditions were observed.  
12      In the grounds for its decision, the Data Protection Board considered that the collection of the data at issue by members of the Jehovah’s Witnesses Community constituted processing of personal data within the meaning of that law, and that the Jehovah’s Witnesses Community and its members were both data controllers.  
13      The Jehovah’s Witnesses Community brought an action before the Helsingin hallinto-oikeus (Administrative Court, Helsinki, Finland) against that decision. By judgment of 18 December 2014, that court annulled the decision on the ground, inter alia, that the Jehovah’s Witnesses Community was not a controller of personal data within the meaning of Law No 523/1999 and that its activity did not constitute unlawful processing of such data.  
14      The Data Protection Supervisor challenged that judgment before the Korkein hallinto-oikeus (Supreme Administrative Court, Finland).  
15      According to the findings of that court, the members of the Jehovah’s Witnesses Community take notes in the course of their door-to-door preaching about visits to persons who are unknown to themselves or that Community. The data collected may consist, among other things, of the name and addresses of persons contacted, together with information concerning their religious beliefs and their family circumstances. Those data are collected as a memory aid and in order to be retrieved for any subsequent visit without the knowledge or consent of the persons concerned.  
16      The referring court also found that the Jehovah’s Witnesses Community has given its members guidelines on the taking of such notes which appear in at least one of its magazines which is dedicated to preaching. That community and its congregations organise and coordinate the door-to-door preaching by their members, in particular by creating maps from which areas are allocated between the members who engage in preaching and by keeping records about preachers and the number of the Community’s publications distributed by them. Furthermore, the congregations of the Jehovah’s Witnesses Community maintain a list of persons who have requested not to receive visits from preachers and the personal data on that list, called the ‘refusal register’, are used by members of that community. Lastly, the Jehovah’s Witnesses Community has, in the past, made forms available to its members for the purpose of collecting those data in the course of their preaching. However, the use of those forms was abandoned following a recommendation by the Data Protection Supervisor.  
17      The referring court observes that, according to information from the Jehovah’s Witnesses Community, it does not require members who engage in preaching to collect data, and that in cases in which such data has been collected it has no knowledge of either the nature of the notes taken which are, moreover, only informal personal notes nor of the identity of the preachers who collected those data.  
18      As regards the need for the present request for a preliminary ruling, the Korkein hallinto-oikeus (Supreme Administrative Court) takes the view that the examination of the case in the main proceedings requires consideration to be given, on one hand, to the rights to privacy and protection of personal data and, on the other, to freedom of religion and association guaranteed by the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms as well as the Finnish Constitution.  
19      The referring court considers that the door-to-door preaching practised by members of a religious community, such as the Jehovah’s Witnesses Community, is not one of the activities excluded from the scope of Directive 95/46, by virtue of the first indent of Article 3(2) thereof. However, the question arises as to whether that activity is a purely personal or household activity within the meaning of the second indent of Article 3(2). In that regard, account must be taken of the fact that, in the present case, the data collected are more than informal notes in an address book, as the notes taken concern unknown persons and contain sensitive data relating to their religious beliefs. The fact that door-to-door preaching is an essential part of the Jehovah’s Witnesses Community’s activity, which is organised and coordinated by it and by its congregations, must also be taken into consideration.  
20      Furthermore, since the collected data at issue in the main proceedings are processed otherwise than by automatic means, it must be determined, having regard to Article 3(1) of Directive 95/46 read together with Article 2(c) thereof, whether that set of data constitutes a filing system within the meaning of those provisions. According to the information provided by the Jehovah’s Witnesses Community, those data are not shared, so that it is impossible to know with certainty the nature and extent of the data collected. However, it may be assumed that the purpose of collecting and subsequent processing of the data at issue in the main proceedings is for the easy retrieval of that data concerning a specific person or address for the purposes of a subsequent visit. The data collected are not, however, structured in the form of data sheets.  
21      If the data processing at issue in the main proceedings falls within the scope of Directive 95/46, the referring court notes that the question then arises as to whether the Jehovah’s Witnesses Community must be regarded as a controller of that processing within the meaning of Article 2(d) thereof. The case-law of the Court deriving from the judgment of 13 May 2014,   
Google Spain and Google  
 (C-131/12, EU:C:2014:317), broadly defines the concept of ‘controller’ within the meaning of those provisions. Furthermore, it is clear from Opinion 1/2010 of 16 February 2010 on the concepts of ‘controller’ and ‘processor’ produced by the Working Group set up pursuant to Article 29 of Directive 95/46, that, in particular, the ‘effective control’ and the conception that the data subject has of the controller must be taken into account.  
22      In the present case, regard should be had to the fact that the Jehovah’s Witnesses Community organises, coordinates and encourages door-to-door preaching, and that in its publications it has given guidelines on the collection of data in the course of that activity. Furthermore, the Data Protection Supervisor found that that community has effective control over the means of data processing and the power to prohibit or limit that processing, and that it previously defined the purpose and means of data collection by giving guidelines on collection. Furthermore, the forms previously used are also evidence of the active involvement of that community in data processing.  
23      However, account should also be taken of the fact that the members of the Jehovah’s Witnesses Community can decide themselves whether to collect data and to determine the means of doing so. Furthermore, that community does not itself collect data and does not have access to the data collected by its members, except that on the ‘refusal’ list. However, such circumstances do not preclude the potential for several data controllers, each with different roles and responsibilities.  
24      In those circumstances the Korkein hallinto-oikeus (Supreme Administrative Court) decided to stay the proceedings before it and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Must the exceptions to the scope of [Directive 95/46] laid down in Article 3(2), first and second indents, thereof be interpreted as meaning that the collection and other processing of personal data carried out by the members of a religious community in connection with door-to-door preaching fall outside the scope of that directive? When assessing the applicability of [Directive 95/46], what significance is to be given, on one hand, to the fact that it is the religious community and its congregations which organise the preaching activity in the course of which the data is collected and, on the other, to the fact this also concerns the personal religious practice of the members of a religious community?  
(2)      Must the definition of a “filing system” in Article 2(c) of … Directive [95/46], examined in the light of recitals 26 and 27 of that directive, be interpreted as meaning that, taken as a whole, the personal data (consisting of names and addresses and other information about and characteristics of a person) collected otherwise than by automatic means in connection with the door-to-door preaching described above  
(a)      does not constitute such a filing system, because the data does not include specific lists or data sheets or any other comparable search method as provided for in the definition laid down in the [Law No 523/1999], or  
(b)      does constitute such a filing system, because, taking account of its intended purpose, the information required for later use may in practice be searched easily and without unreasonable expense in accordance with [Law No 523/1999]?  
(3)      Must the phrase “alone or jointly with others determines the purposes and means of the processing of personal data” appearing in Article 2(d) of … Directive [95/46] be interpreted as meaning that a religious community that organises an activity in the course of which personal data is collected (in particular, by allocating areas in which the activity is carried out among the various preachers, supervising the activity of those preachers and keeping a list of individuals who do not wish the preachers to visit them) may be regarded as a controller, in respect of the processing of personal data carried out by its members, even if the religious community claims that only the individual members who engage in preaching have access to the data that they gather?  
(4)      Must Article 2(d) of Directive [95/46] be interpreted to the effect that in order for a religious community to be considered a controller it must have taken other specific measures, such as giving written instructions or orders directing the collection of data, or is it sufficient that that religious community can be regarded as having de facto control of its members’ activities?  
It is necessary to answer Questions 3 and 4 only if, on the basis of the answers to Questions 1 and 2, [Directive 95/46] is applicable. It is necessary to answer Question 4 only if, on the basis of Question 3, the application of Article 2(d) of [Directive 95/46] to the Community cannot be regarded as being excluded.’  
   
The request to have the oral procedure reopened  
25      By two documents lodged at the Court Registry on 12 December 2017 and 15 February 2018 respectively, the Jehovah’s Witnesses Community requested the Court to order the reopening of the oral part of the procedure pursuant to Article 83 of the Rules of Procedure of the Court. In support of the first of those requests, the Jehovah’s Witnesses Community claims, in particular, that it did not have the opportunity at the hearing to respond to the observations submitted by the other parties, some of which did not reflect the facts in the main proceedings. As regards the second request, the Jehovah’s Witnesses Community argues essentially that the Opinion of the Advocate General is based on inaccurate or potentially misleading facts, some of which are not mentioned in the request for a preliminary ruling.  
26      Pursuant to Article 83 of its Rules of Procedure, the Court may at any time, after hearing the Advocate General, order the reopening of the oral part of the procedure, in particular if it considers that it lacks sufficient information or where a party has, after the close of that part of the procedure, submitted a new fact which is of such a nature as to have a decisive bearing on the decision of the Court, or where the case must be decided on the basis of an argument which has not been debated between the parties or the interested persons referred to in Article 23 of the Statute of the Court of Justice of the European Union.  
27      That is not the case here. In particular, the requests of the Jehovah’s Witnesses Community seeking to have the oral procedure reopened do not contain any new argument on the basis of which the present case should be decided. Furthermore, that party and the other interested parties referred to in Article 23 of the Statute of the Court of Justice of the European Union submitted, both during the written phase and the oral phase of the proceedings, their observations concerning the interpretation of Article 2(c) and (d), and Article 3 of Directive 95/46, read in the light of Article 10 of the Charter, which is the subject of the questions referred for a preliminary ruling.  
28      As regards the facts in the main proceedings, it must be recalled that in proceedings under Article 267 TFEU, only the court making the reference may define the factual context in which the questions which it asks arise or, at very least, explain the factual assumptions on which the questions are based. It follows that a party to the main proceedings cannot allege that certain factual premisses on which the arguments advanced by the other interested parties referred to in Article 23 of the Statute of the Court of Justice of the European Union are based, or the analysis of the Advocate General, are incorrect in order to justify the reopening of the oral procedure, on the basis of Article 83 of the Rules of Procedure (see, to that effect, judgment of 26 June 2008,   
Burda  
, C-284/06, EU:C:2008:365, paragraphs 44, 45 and 47).  
29      Against that background, the Court, having heard the Advocate General, considers that it has all the evidence necessary to enable it to reply to the questions referred and that the present case does not thereby fall to be decided on the basis of an argument which has not been debated between the parties. The request to reopen the oral procedure must therefore be rejected.  
   
Admissibility of the request for a preliminary ruling  
30      The Jehovah’s Witnesses Community claims that the request for a preliminary ruling is inadmissible. While challenging the main facts on which that request is based, it claims that the request for a preliminary ruling relates to the conduct of some of its members who are not parties to the main proceedings. Therefore, that request concerns a hypothetical problem.  
31      In that connection, it is solely for the national court hearing the case, which has the responsibility of taking the subsequent judicial decision, to determine, with regard to the particular aspects of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it refers to the Court. Consequently, where the questions put by national courts concern the interpretation of a provision of European Union law, the Court is, in principle, bound to give a ruling. The Court may refuse to rule on a question referred by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see, to that effect, judgment of 27 June 2017,   
Congregación de Escuelas Pías Provincia Betania  
, C-74/16, EU:C:2017:496, paragraphs 24 and 25 and the case-law cited).  
32      In the present case, the order for reference contains sufficient factual and legal information to understand both the questions referred for a preliminary ruling and their scope. Further, and most importantly, nothing in the file leads to the conclusion that the interpretation requested of EU law is unrelated to the actual facts of the main action or its object, or that the problem is hypothetical, in particular on account of the fact that the members of the Jehovah’s Witnesses Community whose collection of personal data is the basis for the questions referred are not parties to the main proceedings. It is clear from the order for reference that the questions referred are intended to assist the referring court to determine whether that community may itself be regarded as a controller, within the meaning of Directive 95/46, in connection with the collection of the personal data by its members in the course of their door-to-door preaching activities.  
33      The reference for a preliminary ruling is therefore admissible.  
   
Consideration of the questions referred  
   
The first question  
34      By its first question, the referring court asks essentially whether Article 3(2) of Directive 95/46, read in the light of Article 10(1) of the Charter, must be interpreted as meaning that the collection of personal data by members of a religious community in the course of door-to-door preaching and the subsequent processing of those data constitutes the processing of personal data carried out for the purposes of the activities referred to in Article 3(2), first indent, of that directive or the processing of personal data carried out by a natural person in the course of a purely personal or household activity within the meaning of Article 3(2), second indent, thereof.  
35      In order to answer that question, it should be observed from the outset, as is clear from Article 1(1) and recital 10 of Directive 95/46, that that directive seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (judgments of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 66, and of 5 June 2018,   
Wirtshaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 26).  
36      Article 3 of Directive 95/46, which defines the scope of the directive, states in paragraph 1 that its provisions ‘shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system’.  
37      However, Article 3(2) lays down two exceptions to the scope of application of that directive which must be strictly interpreted (see, to that effect, judgments of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraph 29, and of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraph 38). Furthermore, Directive 95/46 does not lay down any further limitation of its scope (judgment of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 46).  
38      First, as regards the exception in Article 3(2), first indent, of Directive 95/46, it has been held that the activities mentioned therein by way of exceptions are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active. Those activities are intended to define the scope of the exception provided for in that provision, with the result that that exception applies only to the activities which are expressly listed there or which can be classified in the same category (judgments of 6 November 2003,   
Lindqist  
, C-101/01, EU:C:2003:596, paragraphs 43 and 44; of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 41; and of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraphs 36 and 37).  
39      In the present case, the collection of personal data by members of the Jehovah’s Witnesses Community in the course of door-to-door preaching is a religious procedure carried out by individuals. It follows that such activity is not an activity of the State authorities and cannot therefore be treated in the same way as the activities referred to in Article 3(2), first indent, of Directive 95/46.  
40      Second, as regards the exception in Article 3(2), second indent, of Directive 95/46, that provision does not exclude from its scope data processing carried out in relation simply to an activity which is simply a personal or household activity, but only data processing carried out in relation to an activity that is ‘purely’ personal or household in nature (see, to that effect, judgment of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraphs 30).  
41      The words ‘personal or household’, within the meaning of that provision, refer to the activity of the person processing the personal data and not to the person whose data are processed (see, to that effect, judgment of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraphs 31 and 33).  
42      As the Court held, Article 3(2), second indent, of Directive 95/46 must be interpreted as covering only activities that are carried out in the context of the private or family life of individuals. In that connection, an activity cannot be regarded as being purely personal or domestic where its purpose is to make the data collected accessible to an unrestricted number of people or where that activity extends,even partially, to a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner (see, to that effect, judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 47; of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 44; and of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraphs 31 and 33).  
43      In so far as it appears that the personal data processing at issue in the main proceedings is carried out in the course of door-to-door preaching by members of the Jehovah’s Witnesses Community, it must be determined whether such an activity is a purely personal or household activity within the meaning of Article 3(2), second indent, of Directive 95/46.  
44      In that connection, it is clear from the order for reference that door-to-door preaching, in the course of which personal data are collected by members of the Jehovah’s Witnesses Community, is, by its very nature, intended to spread the faith of the Jehovah’s Witnesses Community among people who, as the Advocate General observed in point 40 of his Opinion, do not belong to the faith of the members who engage in preaching. Therefore, that activity is directed outwards from the private setting of the members who engage in preaching.  
45      Furthermore, it is also clear from the order for reference that some of the data collected by the members of that community who engage in preaching are sent by them to the congregations of that community which compile lists from that data of persons who no longer wish to receive visits from those members. Thus, in the course of their preaching, those members make at least some of the data collected accessible to a potentially unlimited number of persons.  
46      As to whether the fact that the processing of personal data is carried out in the course of an activity relating to a religious practice may confer a purely personal or household nature on that door-to-door preaching, it must be recalled that the right to freedom of conscience and religion, enshrined in Article 10(1) of the Charter, implies, in particular, the freedom for everyone to manifest his religion or belief, in worship, teaching, practice and observance.  
47      The Charter adopts a broad understanding of the concept of ‘religion’ in that provision covering both the   
forum internum  
, that is the fact of having a belief, and the   
forum externum  
, that is the manifestation of religious faith in public (judgment of 29 May 2018,   
Liga van Moskeeën en Islamitische Organisaties Provincie Antwerpen VZW and Others  
, C-426/16, EU:C:2018:335, paragraph 44 and the case-law cited).  
48      Furthermore, the freedom to manifest one’s religion individually or collectively in public or in private, since it may take various forms such as the teaching, practice and performance of rites, includes also the right to attempt to convince other persons, for example by means of preaching (ECtHR, 25 May 1993,   
Kokkinakis  
v. Greece  
, EC:ECHR:1993:0525JUD001430788, § 31, and ECtHR, 8 November 2007,   
Perry v. Latvia  
, CE:ECHR:2007:1108JUD003027303, § 52).  
49      However, although the door-to-door preaching activities of the member of a religious community is thereby protected by Article 10(1) of the Charter as an expression of the faith of those preachers, that fact does not confer an exclusively personal or household character on that activity, within the meaning of Article 3(2), second indent, of Directive 95/46.  
50      Taking account of the considerations set out in paragraphs 44 and 45 of the present judgment, the preaching extends beyond the private sphere of a member of a religious community who is a preacher.  
51      Having regard to the foregoing considerations, the answer to Question 1 is that Article 3(2) of Directive 95/46, read in the light of Article 10(1) of the Charter, must be interpreted as meaning that the collection of personal data by members of a religious community in the course of door-to-door preaching and the subsequent processing of those data does not constitute either the processing of personal data for the purpose of activities referred to in Article 3(2), first indent, of that directive or the processing of personal data carried out by a natural person in the course of a purely personal or household activity, within the meaning of Article 3(2), second indent, thereof.  
   
The second question  
52      By its second question, the referring court asks essentially whether Article 2(c) of Directive 95/46 must be interpreted as meaning that the concept of a ‘filing system’ referred to in that provision covers a set of personal data collected in the course of door-to-door preaching, consisting of names and addresses as well as other information concerning persons contacted, if those data may, in practice, be easily retrieved for later use, or whether, in order to be covered by that definition, that set of data must include data sheets, specific lists or other search methods.  
53      As is clear from Article 3(1) and recitals 15 and 27 of Directive 95/46, that directive covers both automatic processing of data and the manual processing of such data, so that the scope of the protection it confers on data subjects does not depend on the techniques used and avoids the risk of that protection being circumvented. However, it is also clear that that directive applies to the manual processing of personal data only where the data processed form part of a filing system or are intended to form part of a filing system.  
54      In the present case, since the processing of the personal data at issue in the main proceedings is carried out otherwise than by automatic means, the question arises as to whether the data processed form part of or are intended to form part of a filing system within the meaning of Article 2(c) and Article 3(1) of Directive 95/46.  
55      In that connection, it is stipulated in Article 2(c) of Directive 95/46 that the concept of a ‘filing system’ is ‘any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis’.  
56      In accordance with the objective set out in paragraph 53 of the present judgment, that provision broadly defines the concept of ‘filing system’, in particular by referring to ‘any’ structured set of personal data.  
57      As is clear from recitals 15 and 27 of Directive 95/46, the content of a filing system must be structured in order to allow easy access to personal data. Furthermore, although Article 2(c) of that directive does not set out the criteria according to which that filing system must be structured, it is clear from those recitals that those criteria must be ‘relat[ed] to individuals’. Therefore, it appears that the requirement that the set of personal data must be ‘structured according to specific criteria’ is simply intended to enable personal data to be easily retrieved.  
58      Apart from that requirement, Article 2(c) of Directive 95/46 does not lay down the practical means by which a filing system is be structured or the form in which it is to be presented. In particular, it does not follow from that provision, or from any other provision of that directive, that the personal data at issue must be contained in data sheets or specific lists or in another search method, in order to establish the existence of a filing system within the meaning of that directive.  
59      In the present case, it is clear from the findings of the referring court that the data collected in the course of the door-to-door preaching at issue in the main proceedings are collected as a memory aid, on the basis of an allocation by geographical sector, in order to facilitate the organisation of subsequent visits to persons who have already been contacted. They include not only information relating to the content of conversations concerning the beliefs of the person contacted, but also his name and address. Furthermore, those data, or at least a part of them, are used to draw up lists kept by the congregations of the Jehovah’s Witnesses Community of persons who no longer wish to receive visits by members who engage in the preaching of that community.  
60      Thus, it appears that the personal data collected in the course of the door-to-door preaching at issue in the main proceedings are structured according to criteria chosen in accordance with the objective pursued by that collection, which is to prepare for subsequent visits and to keep lists of persons who no longer wish to be contacted. Thus, as it is apparent from the order for reference, those criteria, among which are the name and address of persons contacted, their beliefs or their wish not to receive further visits, are chosen so that they enable data relating to specific persons to be easily retrieved.  
61      In that connection, the specific criterion and the specific form in which the set of personal data collected by each of the members who engage in preaching is actually structured is irrelevant, so long as that set of data makes it possible for the data relating to a specific person who has been contacted to be easily retrieved, which is however for the referring court to ascertain in the light of all the circumstances of the case in the main proceedings.  
62      Therefore, the answer to Question 2 is that Article 2(c) of Directive 95/46 must be interpreted as meaning that the concept of a ‘filing system’, referred to by that provision, covers a set of personal data collected in the course of door-to-door preaching, consisting of the names and addresses and other information concerning the persons contacted, if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use. In order for such a set of data to fall within that concept, it is not necessary that they include data sheets, specific lists or other search methods.  
   
The third and fourth questions  
63      By Questions 3 and 4, which it is appropriate to examine together, the referring court asks essentially whether Article 2(d) of Directive 95/46, read in the light of Article 10(1) of the Charter, must be interpreted as meaning that a religious community may be regarded as a controller, jointly with its members who engage in preaching, with regard to the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, and whether it is necessary for that purpose for the community to have access to those data, or whether it must be established that the religious community has given its members written guidelines or instructions in relation to that processing.  
64      In the present case, the Data Protection Board, in the decision at issue in the main proceedings, found that the Jehovah’s Witnesses Community is a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching. In so far as only the responsibility of that community is challenged, the responsibility of the members who engage in preaching does not appear to be called into question.  
65      As expressly provided in Article 2(d) of Directive 95/46, the concept of ‘controller’ refers to the natural or legal person who ‘alone or jointly with others determines the purposes and means of the processing of personal data’. Therefore, that concept does not necessarily refer to a single natural or legal person and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions (see, to that effect, judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 29).  
66      The objective of that provision being to ensure, through a broad definition of the concept of ‘controller’, effective and complete protection of the persons concerned, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case (see, to that effect, judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraphs 28, 43 and 44).  
67      In that connection, neither the wording of Article 2(d) of Directive 95/46 nor any other provision of that directive supports a finding that the determination of the purpose and means of processing must be carried out by the use of written guidelines or instructions from the controller.  
68      However, a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46.  
69      Furthermore, the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned (see, to that effect, judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 38).  
70      In the present case, as is clear from the order for reference, it is true that members of the Jehovah’s Witnesses Community who engage in preaching determine in which specific circumstances they collect personal data relating to persons visited, which specific data are collected and how those data are subsequently processed. However, as set out in paragraphs 43 and 44 of the present judgment, the collection of personal data is carried out in the course of door-to-door preaching, by which members of the Jehovah’s Witnesses Community who engage in preaching spread the faith of their community. That preaching activity is, as is apparent from the order for reference, organised, coordinated and encouraged by that community. In that context, the data are collected as a memory aid for later use and for a possible subsequent visit. Finally, the congregations of the Jehovah’s Witnesses Community keep lists of persons who no longer wish to receive a visit, from those data which are transmitted to them by members who engage in preaching.  
71      Thus, it appears that the collection of personal data relating to persons contacted and their subsequent processing help to achieve the objective of the Jehovah’s Witnesses Community, which is to spread its faith and are, therefore, carried out by members who engage in preaching for the purposes of that community. Furthermore, not only does the Jehovah’s Witnesses Community have knowledge on a general level of the fact that such processing is carried out in order to spread its faith, but that community organises and coordinates the preaching activities of its members, in particular, by allocating areas of activity between the various members who engage in preaching.  
72      Such circumstances lead to the conclusion that the Jehovah’s Witnesses Community encourages its members who engage in preaching to carry out data processing in the context of their preaching activity.  
73      In the light of the file submitted to the Court, it appears that the Jehovah’s Witnesses Community, by organising, coordinating and encouraging the preaching activities of its members intended to spread its faith, participates, jointly with its members who engage in preaching, in determining the purposes and means of processing of personal data of the persons contacted, which is, however, for the referring court to verify with regard to all of the circumstances of the case.  
74      That finding cannot be called into question by the principle of organisational autonomy of religious communities which derives from Article 17 TFEU. The obligation for every person to comply with the rules of EU law on the protection of personal data cannot be regarded as an interference in the organisational autonomy of those communities (see, to that effect, judgment of 17 April 2018,   
Egenberger  
, C-414/16, EU:C:2018:257, paragraph 58).  
75      Having regard to the foregoing considerations, the answer to Questions 3 and 4 is that Article 2(d) of Directive 95/46, read in the light of Article 10(1) of the Charter, must be interpreted as meaning that it supports the finding that a religious community is a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data, or to establish that that community has given its members written guidelines or instructions in relation to the data processing.  
   
Costs  
76      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 3(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, read in the light of Article 10(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that the collection of personal data by members of a religious community in the course of door-to-door preaching and the subsequent processing of those data does not constitute either the processing of personal data for the purpose of activities referred to in Article 3(2), first indent, of that directive or the processing of personal data carried out by a natural person in the course of a purely personal or household activity, within the meaning of Article 3(2), second indent, thereof.  
2.        
Article 2(c) of Directive 95/46 must be interpreted as meaning that the concept of a ‘filing system’, referred to by that provision, covers a set of personal data collected in the course of door-to-door preaching, consisting of the names and addresses and other information concerning the persons contacted, if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use. In order for such a set of data to fall within that concept, it is not necessary that they include data sheets, specific lists or other search methods.  
3.        
Article 2(d) of Directive 95/46, read in the light of Article 10(1) of the Charter of Fundamental Rights, must be interpreted as meaning that it supports the finding that a religious community is a controller, jointly with its members who engage in preaching, for the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data, or to establish that that community has given its members written guidelines or instructions in relation to the data processing.

ID: 37c4644a-6ef7-4c73-ab91-cf1c1f360c79

Judgment of 5 Jun 2018, C-210/16 (  
Wirtschaftsakademie Schleswig-Holstein  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Joint controllers   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Territorial Scope   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Main Establishment   
General data protection law   
 >   
Chapter VII - Cooperation and consistency   
   
JUDGMENT OF THE COURT (Grand Chamber)  
5 June 2018 (\*)  
(Reference for a preliminary ruling — Directive 95/46/EC — Personal data — Protection of natural persons with respect to the processing of that data — Order to deactivate a Facebook page (fan page) enabling the collection and processing of certain data of visitors to that page — Article 2(d) — Controller responsible for the processing of personal data — Article 4 — Applicable national law — Article 28 — National supervisory authorities — Powers of intervention of those authorities)  
In Case C-210/16,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Germany), made by decision of 25 February 2016, received at the Court on 14 April 2016, in the proceedings  
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein  
v  
Wirtschaftsakademie Schleswig-Holstein GmbH,  
interveners:  
Facebook Ireland Ltd,  
Vertreter des Bundesinteresses beim Bundesverwaltungsgericht,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Tizzano (Rapporteur), Vice-President, M. Ilešič, L. Bay Larsen, T. von Danwitz, A. Rosas, J. Malenovský and E. Levits, Presidents of Chambers, E. Juhász, A. Borg Barthet, F. Biltgen, K. Jürimäe, C. Lycourgos, M. Vilaras and E. Regan, Judges,  
Advocate General: Y. Bot,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 27 June 2017,  
after considering the observations submitted on behalf of:  
–        Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, by U. Karpenstein and M. Kottmann, Rechtsanwälte,  
–        Wirtschaftsakademie Schleswig-Holstein GmbH, by C. Wolff, Rechtsanwalt,  
–        Facebook Ireland Ltd, by C. Eggers, H.-G. Kamann and M. Braun, Rechtsanwälte, and I. Perego, avvocato,  
–        the German Government, by J. Möller, acting as Agent,  
–        the Belgian Government, by L. Van den Broeck, C. Pochet, P. Cottin and J.-C. Halleux, acting as Agents,  
–        the Czech Government, by M. Smolek, J. Vláčil and L. Březinová, acting as Agents,  
–        Ireland, by M. Browne, L. Williams, E. Creedon, G. Gilmore and A. Joyce, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,  
–        the Netherlands Government, by C.S. Schillemans and K. Bulterman, acting as Agents,  
–        the Finnish Government, by J. Heliskoski, acting as Agent,  
–        the European Commission, by H. Krämer and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 24 October 2017,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent Data Protection Centre for the   
Land  
 of Schleswig-Holstein, Germany) (‘the ULD’) and Wirtschaftsakademie Schleswig-Holstein GmbH, a private-law company operating in the field of education (‘Wirtschaftsakademie’), concerning the lawfulness of ULD’s order to Wirtschaftsakademie to deactivate its fan page on the Facebook social network site (‘Facebook’).  
   
Legal context  
   
EU law  
3        Recitals 10, 18, 19 and 26 of Directive 95/46 state:  
‘(10)      Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of [EU] law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the [European Union];  
...  
(18)      Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the [European Union] must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;  
(19)      Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;  
…  
(26)      Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; …’  
4        Article 1 of Directive 95/46, ‘Object of the Directive’, provides:  
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
5        Article 2 of Directive 95/46, ‘Definitions’, reads as follows:  
‘For the purposes of this Directive:  
…  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
...  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or [EU] laws or regulations, the controller or the specific criteria for his nomination may be designated by national or [EU] law;  
(e)      “processor” shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;  
(f)      “third party” shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;  
...’  
6        Article 4 of that directive, ‘National law applicable’, provides in paragraph 1:  
‘Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:  
(a)      the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;  
(b)      the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;  
(c)      the controller is not established on [EU] territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the [European Union].’  
7        Article 17 of the directive, ‘Security of processing’, provides in paragraphs 1 and 2:   
‘1.      Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.  
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.  
2.      The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.’  
8        Article 24 of the directive, ‘Sanctions’, provides:  
‘The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.’  
9        Article 28 of the directive, ‘Supervisory authority’, reads as follows:  
‘1.      Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.  
These authorities shall act with complete independence in exercising the functions entrusted to them.  
2.      Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals’ rights and freedoms with regard to the processing of personal data.  
3.      Each authority shall in particular be endowed with:  
–        investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,  
–        effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,  
–        the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.  
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.  
...  
6.      Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.  
The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.  
...’  
   
German law  
10      Paragraph 3(7) of the Bundesdatenschutzgesetz (Federal Law on data protection), in the version applicable to the main proceedings (‘the BDSG’), reads as follows:   
‘A responsible entity is any person or entity which collects, processes or uses personal data on its own behalf, or commissions others to do this.’  
11      Paragraph 11 of the BDSG, ‘Collection, processing or use of personal data by entities commissioned’, reads:  
‘(1)      If personal data is collected, processed or used by other entities commissioned to do so, the commissioning entity is responsible for compliance with the provisions of this law and with other provisions on data protection. …  
(2)      The entity commissioned must be selected carefully with particular account being taken of the suitability of the technical and organisational measures taken by it. The commission must be given in writing, with the following in particular being determined in detail: …   
The commissioning entity must satisfy itself, before the start of the data processing and regularly thereafter, that the technical and organisational measures taken by the entity commissioned are complied with. The results must be documented.  
…’  
12      Paragraph 38(5) of the BDSG provides:  
‘To ensure compliance with this law and with other provisions on data protection, the supervisory authority may order measures to eliminate breaches that have been ascertained in the collection, processing or use of personal data or technical or organisational defects. In the case of serious breaches or defects, in particular those which are associated with a particular threat to the right to protection of personality, it can prohibit the collection, processing or use or the application of specific procedures if the breaches or defects are not eliminated within a reasonable time, contrary to an order in accordance with the first sentence and despite the imposition of a penalty payment. It can require the data protection officer to be removed if he does not possess the expert knowledge and reliability needed to perform his duties.’  
13      Paragraph 12 of the Telemediengesetz (Law on electronic media) of 26 February 2007 (BGBl. 2007 I, p. 179, ‘the TMG’) reads as follows:  
‘(1)      The service provider may collect and use personal data for the provision of electronic media only where this law or another provision of law expressly relating to electronic media permits it or the user has consented.  
...   
(3)      Except as provided otherwise, the provisions in force for the protection of personal data are to be applied even if the data is not processed automatically.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
14      Wirtschaftsakademie offers educational services by means of a fan page hosted on Facebook.  
15      Fan pages are user accounts that can be set up on Facebook by individuals or businesses. To do so, the author of the fan page, after registering with Facebook, can use the platform designed by Facebook to introduce himself to the users of that social network and to persons visiting the fan page, and to post any kind of communication in the media and opinion market. Administrators of fan pages can obtain anonymous statistical information on visitors to the fan pages via a function called ‘Facebook Insights’ which Facebook makes available to them free of charge under non-negotiable conditions of use. That information is collected by means of evidence files (‘cookies’), each containing a unique user code, which are active for two years and are stored by Facebook on the hard disk of the computer or on other media of visitors to fan pages. The user code, which can be matched with the connection data of users registered on Facebook, is collected and processed when the fan pages are opened. According to the order for reference, neither Wirtschaftsakademie nor Facebook Ireland Ltd notified the storage and functioning of the cookie or the subsequent processing of the data, at least during the material period for the main proceedings.  
16      By decision of 3 November 2011 (‘the contested decision’), the ULD, as supervisory authority within the meaning of Article 28 of Directive 95/46, with the task of supervising the application in the   
Land  
 of Schleswig-Holstein (Germany) of the provisions adopted by the Federal Republic of Germany pursuant to that directive, ordered Wirtschaftsakademie, in accordance with the first sentence of Paragraph 38(5) of the BDSG, to deactivate the fan page it had set up on Facebook at the address www.facebook.com/wirtschaftsakademie, on pain of a penalty payment if it failed to comply within the prescribed period, on the ground that neither Wirtschaftsakademie nor Facebook informed visitors to the fan page that Facebook, by means of cookies, collected personal data concerning them and then processed the data. Wirtschaftsakademie brought a complaint against that decision, arguing essentially that it was not responsible under data protection law for the processing of the data by Facebook or the cookies which Facebook installed.  
17      By decision of 16 December 2011, the ULD dismissed the complaint, finding that Wirtschaftsakademie as a service provider was liable under Paragraph 3(3)(4) and Paragraph 12(1) of the TMG in conjunction with Paragraph 3(7) of the BDSG. The ULD stated that, by setting up its fan page, Wirtschaftsakademie had made an active and deliberate contribution to the collection by Facebook of personal data relating to visitors to the fan page, from which it profited by means of the statistics provided to it by Facebook.  
18      Wirtschaftsakademie brought an action against that decision in the Verwaltungsgericht (Administrative Court, Germany), submitting that the processing of personal data by Facebook could not be attributed to it and that it had not commissioned Facebook within the meaning of Paragraph 11 of the BDSG to process data that it controlled or was able to influence. Wirtschaftsakademie concluded that the ULD should have acted directly against Facebook instead of adopting the contested decision against it.  
19      By judgment of 9 October 2013, the Verwaltungsgericht (Administrative Court) annulled the contested decision, essentially on the ground that, since the administrator of a fan page on Facebook is not a responsible entity within the meaning of Paragraph 3(7) of the BDSG, Wirtschaftsakademie could not be the addressee of a measure taken under Paragraph 38(5) of the BDSG.  
20      The Oberverwaltungsgericht (Higher Administrative Court, Germany) dismissed the ULD’s appeal against that judgment as unfounded. It found essentially that the prohibition of the processing of data in the contested decision was unlawful, in that the second sentence of Paragraph 38(5) of the BDSG lays down a step-by-step procedure whose first step allows only the adoption of measures for the elimination of infringements that have been ascertained in the processing of data. An immediate prohibition of the processing of data comes into consideration only if a data processing procedure is unlawful in its entirety and the only possible remedy is to terminate it. According to the Oberverwaltungsgericht (Higher Administrative Court), that was not the case here, since it would have been possible for Facebook to put an end to the infringements alleged by the ULD.  
21      The Oberverwaltungsgericht (Higher Administrative Court) further stated that the contested decision was also unlawful on the ground that an order under Paragraph 38(5) of the BDSG may only be made against the responsible entity within the meaning of Paragraph 3(7) of the BDSG, and that Wirtschaftsakademie was not such an entity in relation to the data collected by Facebook. Facebook alone decided on the purpose and means of collecting and processing personal data used for the Facebook Insights function, Wirtschaftsakademie receiving only anonymised statistical information.  
22      The ULD appealed on a point of law to the Bundesverwaltungsgericht (Federal Administrative Court, Germany), relying inter alia on an infringement of Paragraph 38(5) of the BDSG and on a number of procedural errors vitiating the appellate court’s decision. It considers that the infringement committed by Wirtschaftsakademie consisted in commissioning an inappropriate supplier — inappropriate because it did not comply with the applicable data protection law — namely Facebook Ireland, to create, host and maintain a website. The order to Wirtschaftsakademie to deactivate its fan page, imposed by the contested decision, was thus intended to remedy that breach, since it prohibited it from continuing to make use of Facebook infrastructure as the technical basis of its website.  
23      Like the Oberverwaltungsgericht (Higher Administrative Court), the Bundesverwaltungsgericht (Federal Administrative Court) takes the view that Wirtschaftsakademie cannot itself be regarded as responsible for the data processing within the meaning Paragraph 3(7) of the BDSG or Article 2(d) of Directive 95/46. It considers nevertheless that the concept of controller should in principle be interpreted broadly, in the interests of effective protection of the right of privacy, as the Court has held in its recent case-law on the point. It further entertains doubts as to the powers of the ULD with respect to Facebook Germany in the present case, given that it is Facebook Ireland that is responsible, at EU level, for the collection and processing of personal data within the Facebook group. Finally, it is uncertain as to the effect, for the purpose of the exercise of the ULD’s powers of intervention, of the assessments made by the supervisory authority to which Facebook Ireland is subject concerning the lawfulness of the processing of personal data at issue.  
24      In those circumstances, the Bundesverwaltungsgericht (Federal Administrative Court) decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Is Article 2(d) of Directive [95/46] to be interpreted as definitively and exhaustively defining the liability and responsibility for data protection infringements, or does scope remain, under the “suitable measures” pursuant to Article 24 of Directive [95/46] and the “effective powers of intervention” pursuant to the second indent of Article 28(3) of Directive [95/46], in multi-tiered information provider relationships, for responsibility of an entity that does not control the data processing within the meaning of Article 2(d) of Directive [95/46] when it chooses the operator of its information offering?  
(2)      Does it follow   
a contrario  
 from the obligation of Member States under Article 17(2) of Directive [95/46] to provide, where data processing is carried out on the controller’s behalf, that the controller must “choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out”, that, where there are other user relationships not linked to data processing on the controller’s behalf within the meaning of Article 2(e) of Directive [95/46], there is no obligation to make a careful selection and no such obligation can be based on national law?  
(3)      In cases in which a parent company based outside the European Union has legally independent establishments (subsidiaries) in various Member States, is the supervisory authority of a Member State (in this case, Germany) entitled under Article 4 and Article 28(6) of Directive [95/46] to exercise the powers conferred under Article 28(3) of Directive [95/46] against the establishment located in its territory even when this establishment is responsible solely for promoting the sale of advertising and other marketing measures aimed at the inhabitants of that Member State, whereas the independent establishment (subsidiary) located in another Member State (in this case, Ireland) is exclusively responsible within the group’s internal division of tasks for collecting and processing personal data throughout the entire territory of the European Union and hence in the other Member State as well (in this case, Germany), if the decision on the data processing is in fact taken by the parent company?  
(4)      Are Article 4(1)(a) and Article 28(3) of Directive [95/46] to be interpreted as meaning that, in cases in which the controller has an establishment in the territory of one Member State (in this case, Ireland) and there is another, legally independent establishment in the territory of another Member State (in this case, Germany), whose responsibilities include the sale of advertising space and whose activity is aimed at the inhabitants of that State, the competent supervisory authority in this other Member State (in this case, Germany) may direct measures and orders implementing data protection legislation also against the other establishment (in this case, in Germany) not responsible for data processing under the group’s internal division of tasks and responsibilities, or are measures and orders only possible by the supervisory body of the Member State (in this case, Ireland) in whose territory the entity with internal responsibility within the group has its registered office?  
(5)      Are Article 4(1)(a) and Article 28(3) and (6) of Directive [95/46] to be interpreted as meaning that, in cases in which the supervisory authority in one Member State (in this case, Germany) takes action against a person or entity in its territory pursuant to Article 28(3) of Directive [95/46] on the grounds of failure carefully to select a third party involved in the data processing process (in this case, Facebook), because that third party infringes data protection legislation, the active supervisory authority (in this case, Germany) is bound by the appraisal made under data protection legislation by the supervisory authority of the Member State in which the third party responsible for the data processing has its establishment (in this case, Ireland) meaning that it may not arrive at a different legal appraisal, or may the active supervisory authority (in this case, Germany) conduct its own examination of the lawfulness of the data processing by the third party established in another Member State (in this case, Ireland) as a preliminary question prior to its own action?  
(6)      If the possibility of conducting an independent examination is available to the active supervisory authority (in this case, Germany), is the second sentence of Article 28(6) of Directive [95/46] to be interpreted as meaning that this supervisory authority may exercise the effective powers of intervention conferred on it under Article 28(3) of Directive [95/46] against a person or entity established in its territory on the grounds of their joint responsibility for data protection infringements by a third party established in another Member State only if and not until it has first requested the supervisory authority in this other Member State (in this case, Ireland) to exercise its powers?’  
   
Consideration of the questions referred  
   
Questions 1 and 2  
25      By its first and second questions, which should be considered together, the referring court essentially wishes to know whether Article 2(d), Article 17(2), Article 24 and the second indent of Article 28(3) of Directive 95/46 must be interpreted as allowing an entity to be held liable in its capacity as administrator of a fan page on a social network where the rules on the protection of personal data are infringed, because it has chosen to make use of that social network to distribute the information it offers.  
26      To answer those questions, it must be recalled that, as is apparent from Article 1(1) and recital 10 of Directive 95/46, the directive aims to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (judgment of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraph 27 and the case-law cited).  
27      In accordance with that aim, Article 2(d) of the directive defines the concept of ‘controller’ broadly as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.  
28      As the Court has previously held, the objective of that provision is to ensure, through a broad definition of the concept of ‘controller’, effective and complete protection of the persons concerned (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 34).  
29      Furthermore, since, as Article 2(d) of Directive 95/46 expressly provides, the concept of ‘controller’ relates to the entity which ‘alone or jointly with others’ determines the purposes and means of the processing of personal data, that concept does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions.  
30      In the present case, Facebook Inc. and, for the European Union, Facebook Ireland must be regarded as primarily determining the purposes and means of processing the personal data of users of Facebook and persons visiting the fan pages hosted on Facebook, and therefore fall within the concept of ‘controller’ within the meaning of Article 2(d) of Directive 95/46, which is not challenged in the present case.  
31      That being so, and in order to answer the questions referred, it must be examined whether and to what extent the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, contributes in the context of that fan page to determining, jointly with Facebook Ireland and Facebook Inc., the purposes and means of processing the personal data of the visitors to the fan page and may therefore also be regarded as a ‘controller’ within the meaning of Article 2(d) of Directive 95/46.  
32      It appears that any person wishing to create a fan page on Facebook concludes a specific contract with Facebook Ireland for the opening of such a page, and thereby subscribes to the conditions of use of the page, including the policy on cookies, which is for the national court to ascertain.  
33      According to the documents before the Court, the data processing at issue in the main proceedings is essentially carried out by Facebook placing cookies on the computer or other device of persons visiting the fan page, whose purpose is to store information on the browsers, those cookies remaining active for two years if not deleted. It also appears that in practice Facebook receives, registers and processes the information stored in the cookies in particular when a person visits ‘the Facebook services, services provided by other members of the Facebook family of companies, and services provided by other companies that use the Facebook services’. Moreover, other entities such as Facebook partners or even third parties ‘may use cookies on the Facebook services to provide services [directly to that social network] and the businesses that advertise on Facebook’.  
34      That processing of personal data is intended in particular to enable Facebook to improve its system of advertising transmitted via its network, and to enable the fan page administrator to obtain statistics produced by Facebook from the visits to the page, for the purposes of managing the promotion of its activity, making it aware, for example, of the profile of the visitors who like its fan page or use its applications, so that it can offer them more relevant content and develop functionalities likely to be of more interest to them.  
35      While the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network, it must be stated, on the other hand, that the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account.  
36      In this context, according to the submissions made to the Court, the creation of a fan page on Facebook involves the definition of parameters by the administrator, depending inter alia on the target audience and the objectives of managing and promoting its activities, which has an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page. The administrator may, with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook. Consequently, the administrator of a fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page.  
37      In particular, the administrator of the fan page can ask for — and thereby request the processing of — demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centres of interest of the target audience and information on the purchases and online purchasing habits of visitors to its page, the categories of goods and services that appeal the most, and geographical data which tell the fan page administrator where to make special offers and where to organise events, and more generally enable it to target best the information it offers.  
38      While the audience statistics compiled by Facebook are indeed transmitted to the fan page administrator only in anonymised form, it remains the case that the production of those statistics is based on the prior collection, by means of cookies installed by Facebook on the computers or other devices of visitors to that page, and the processing of the personal data of those visitors for such statistical purposes. In any event, Directive 95/46 does not, where several operators are jointly responsible for the same processing, require each of them to have access to the personal data concerned.  
39      In those circumstances, the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page. The administrator must therefore be categorised, in the present case, as a controller responsible for that processing within the European Union, jointly with Facebook Ireland, within the meaning of Article 2(d) of Directive 95/46.  
40      The fact that an administrator of a fan page uses the platform provided by Facebook in order to benefit from the associated services cannot exempt it from compliance with its obligations concerning the protection of personal data.  
41      It must be emphasised, moreover, that fan pages hosted on Facebook can also be visited by persons who are not Facebook users and so do not have a user account on that social network. In that case, the fan page administrator’s responsibility for the processing of the personal data of those persons appears to be even greater, as the mere consultation of the home page by visitors automatically starts the processing of their personal data.  
42      In those circumstances, the recognition of joint responsibility of the operator of the social network and the administrator of a fan page hosted on that network in relation to the processing of the personal data of visitors to that page contributes to ensuring more complete protection of the rights of persons visiting a fan page, in accordance with the requirements of Directive 95/46.  
43      However, it should be pointed out, as the Advocate General observes in points 75 and 76 of his Opinion, that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.  
44      In the light of the above considerations, the answer to Questions 1 and 2 is that Article 2(d) of Directive 95/46 must be interpreted as meaning that the concept of ‘controller’ within the meaning of that provision encompasses the administrator of a fan page hosted on a social network.  
   
Questions 3 and 4  
45      By its third and fourth questions, which should be considered together, the referring court essentially wishes to know whether Articles 4 and 28 of Directive 95/46 must be interpreted as meaning that, where an undertaking established outside the European Union has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State, or whether it is for the supervisory authority of that other Member State to exercise those powers with respect to the second establishment.  
46      The ULD and the Italian Government express doubts as to the admissibility of those questions, on the ground that they are not relevant to the outcome of the main proceedings. They submit that the contested decision is addressed to Wirtschaftsakademie and does not therefore concern Facebook Inc. or any of its subsidiaries established in EU territory.  
47      On this point, it must be recalled that, in the context of the cooperation between the Court and the national courts provided for in Article 267 TFEU, it is solely for the national court, before which the dispute has been brought and which must assume responsibility for the subsequent judicial decision, to determine in the light of the particular circumstances of the case both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions submitted concern the interpretation of EU law, the Court is, in principle, bound to give a ruling (judgment of 6 September 2016,   
Petruhhin  
, C-182/15, EU:C:2016:630, paragraph 19 and the case-law cited).  
48      In the present case, it should be noted that the referring court states that an answer by the Court to its third and fourth questions is necessary for it to rule on the main proceedings. It explains that, should it be found in the light of that answer that the ULD could remedy the alleged infringements of the right to protection of personal data by taking a measure against Facebook Germany, such a finding could indicate that the contested decision was vitiated by an error of assessment, in that it was wrongly taken against Wirtschaftsakademie.   
49      In those circumstances, Questions 3 and 4 are admissible.  
50      To answer those questions, it must be recalled as a preliminary point that, in accordance with Article 28(1) and (3) of Directive 95/46, each supervisory authority is to exercise all the powers conferred on it by national law in the territory of its own Member State, in order to ensure compliance with the data protection rules in that territory (see, to that effect, judgment of 1 October 2015,   
Weltimmo  
, C-230/14, EU:C:2015:639, paragraph 51).  
51      The question of which national law applies to the processing of personal data is governed by Article 4 of Directive 95/46. As stated in Article 4(1)(a), each Member State is to apply the national provisions it adopts pursuant to the directive to the processing of personal data, where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. That provision states that, where the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of those establishments complies with the obligations laid down by the national law applicable.  
52      It thus follows from a reading of that provision in conjunction with Article 28(1) and (3) of Directive 95/46 that, where the national law of the Member State of the supervisory authority is applicable under Article 4(1)(a) of the directive because the processing in question is carried out in the context of the activities of an establishment of the controller in the territory of that Member State, that supervisory authority can exercise all the powers conferred on it by that law in respect of that establishment, regardless of whether the controller also has establishments in other Member States.  
53      In order, therefore, to determine whether, in circumstances such as those of the main proceedings, a supervisory authority is entitled to exercise the powers conferred on it by national law against an establishment situated in the territory of its own Member State, it must be ascertained whether the two conditions laid down by Article 4(1)(a) of Directive 95/46 are satisfied, in other words, whether there is an ‘establishment of the controller’ within the meaning of that provision and whether the processing is carried out ‘in the context of the activities’ of the establishment, also within the meaning of that provision.  
54      As regards, first, the condition that the controller responsible for the processing of personal data must have an establishment in the territory of the Member State of the supervisory authority, it must be recalled that, according to recital 19 of Directive 95/46, establishment in the territory of a Member State implies the effective and real exercise of activity through stable arrangements, and the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor (judgment of 1 October 2015,   
Weltimmo  
, C-230/14, EU:C:2015:639, paragraph 28 and the case-law cited).  
55      In the present case, it is common ground that Facebook Inc., as controller jointly responsible with Facebook Ireland for processing personal data, has a permanent establishment in Germany, namely Facebook Germany, situated in Hamburg, and that Facebook Germany effectively and genuinely exercises activities in that Member State. It is therefore an establishment within the meaning of Article 4(1)(a) of Directive 95/46.  
56      As regards, second, the condition that the processing of personal data must be carried out ‘in the context of the activities’ of the establishment in question, it must be recalled, to begin with, that in view of the objective pursued by Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, the expression ‘in the context of the activities of an establishment’ cannot be interpreted restrictively (judgment of 1 October 2015,   
Weltimmo  
, C-230/14, EU:C:2015:639, paragraph 25 and the case-law cited).  
57      Next, it must be pointed out that Article 4(1)(a) of Directive 95/46 does not require that such processing be carried out ‘by’ the establishment concerned itself, but only that it be carried out ‘in the context of the activities of’ the establishment (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 52).  
58      In the present case, the order for reference and the written observations submitted by Facebook Ireland show that Facebook Germany is responsible for promoting and selling advertising space and carries on activities addressed to persons residing in Germany.  
59      As noted in paragraphs 33 and 34 above, the processing of personal data at issue in the main proceedings, carried out by Facebook Inc. jointly with Facebook Ireland, consisting in collecting personal data by means of cookies installed on the computers or other devices of visitors to fan pages hosted on Facebook, is intended, in particular, to enable Facebook to improve its system of advertising, in order better to target its communications.  
60      As the Advocate General observes in point 94 of his Opinion, given that a social network such as Facebook generates a substantial part of its income from advertisements posted on the web pages set up and accessed by users, and given that Facebook’s establishment in Germany is intended to ensure the promotion and sale in Germany of advertising space that makes Facebook’s services profitable, the activities of that establishment must be regarded as inextricably linked to the processing of personal data at issue in the main proceedings, for which Facebook Inc. is jointly responsible with Facebook Ireland. Consequently, such treatment must be regarded as being carried out in the context of the activities of an establishment of the controller within the meaning of Article 4(1)(a) of Directive 95/46 (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraphs 55 and 56).  
61      It follows that, since German law is applicable to the processing of personal data at issue in the main proceedings in accordance with Article 4(1)(a) of Directive 95/46, the German supervisory authority was competent under Article 28(1) of that directive to apply that law to that processing.  
62      That supervisory authority was therefore competent, for the purpose of ensuring compliance in German territory with the rules on the protection of personal data, to exercise with respect to Facebook Germany all the powers conferred on it under the national provisions transposing Article 28(3) of Directive 95/46.  
63      It should also be stated that the circumstance, emphasised by the referring court in its third question, that the strategic decisions on the collection and processing of personal data relating to persons resident in EU territory are taken by a parent company established in a third country, such as Facebook Inc. in the present case, is not capable of calling in question the competence of the supervisory authority operating under the law of a Member State with respect to an establishment in the territory of that State belonging to the controller responsible for the processing of that data.  
64      In the light of the foregoing, the answer to Questions 3 and 4 is that Articles 4 and 28 of Directive 95/46 must be interpreted as meaning that, where an undertaking established outside the European Union has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State.  
   
Questions 5 and 6  
65      By its fifth and sixth questions, which should be considered together, the referring court asks essentially whether Article 4(1)(a) and Article 28(3) and (6) of Directive 95/46 must be interpreted as meaning that, where the supervisory authority of a Member State intends to exercise with respect to an entity established in the territory of that Member State the powers of intervention referred to in Article 28(3) of that directive, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State, that supervisory authority is competent to assess, independently of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene.  
66      To answer those questions, it must be recalled, as may be seen from the answer to the first and second questions referred for a preliminary ruling, that Article 2(d) of Directive 95/46 must be interpreted as allowing, in circumstances such as those of the main proceedings, an entity such as Wirtschaftsakademie to be held responsible, as the administrator of a fan page hosted on Facebook, in the event of an infringement of the rules on the protection of personal data.  
67      It follows that, by virtue of Article 4(1)(a) and Article 28(1) and (3) of Directive 95/46, the supervisory authority of the Member State in whose territory that entity is established is competent to apply its national law, and thus to make use against that entity of all the powers conferred on it by its national law, in accordance with Article 28(3) of that directive.  
68      As provided for by the second subparagraph of Article 28(1) of that directive, the supervisory authorities whose task it is to supervise the application, in the territory of their own Member States, of the provisions adopted by those States pursuant to the directive are to act with complete independence in exercising the functions entrusted to them. That requirement also follows from EU primary law, in particular Article 8(3) of the Charter of Fundamental Rights of the European Union and Article 16(2) TFEU (see, to that effect, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 40).  
69      Furthermore, while under the second subparagraph of Article 28(6) of Directive 95/46 the supervisory authorities are to cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information, that directive does not lay down any criterion of priority governing the intervention of one supervisory authority as against another, nor does it lay down an obligation for a supervisory authority of one Member State to comply with a position which may have been expressed by the supervisory authority of another Member State.  
70      A supervisory authority which is competent under its national law is not therefore obliged to adopt the conclusion reached by another supervisory authority in an analogous situation.  
71      It must be recalled that, as the national supervisory authorities are responsible, in accordance with Article 8(3) of the Charter of Fundamental Rights and Article 28 of Directive 95/46, for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether the processing of personal data in the territory of its own Member State complies with the requirements laid down by Directive 95/46 (see, to that effect, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 47).  
72      Since Article 28 of Directive 95/46 applies by its very nature to any processing of personal data, even where there is a decision of a supervisory authority of another Member State, a supervisory authority hearing a claim lodged by a person concerning the protection of his rights and freedoms with regard to the processing of personal data relating to him must examine, with complete independence, whether the processing of that data complies with the requirements laid down by that directive (see, to that effect, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 57).  
73      It follows that, in the present case, under the system established by Directive 95/46, the ULD was entitled to assess, independently of the assessments made by the Irish supervisory authority, the lawfulness of the data processing at issue in the main proceedings.  
74      Consequently, the answer to Questions 5 and 6 is that Article 4(1)(a) and Article 28(3) and (6) of Directive 95/46 must be interpreted as meaning that, where the supervisory authority of a Member State intends to exercise with respect to an entity established in the territory of that Member State the powers of intervention referred to in Article 28(3) of that directive, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State, that supervisory authority is competent to assess, independently of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene.  
   
Costs  
75      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 2(d) of Directive   
95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data   
must be interpreted as meaning that the concept of ‘controller’ within the meaning of that provision encompasses the administrator of a fan page hosted on a social network.  
2.        
Articles 4 and 28 of Directive 95/46 must be interpreted as meaning that, where an undertaking established outside the European Union has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State.  
3.        
Article 4(1)(a) and Article 28(3) and (6) of Directive 95/46 must be interpreted as meaning that, where the supervisory authority of a Member State intends to exercise with respect to an entity established in the territory of that Member State the powers of intervention referred to in Article 28(3) of that directive, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State, that supervisory authority is competent to assess, independently of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene.

ID: 398f73a8-d6d2-425e-ab4c-4e0cfd441a46

of 15 Jun 2021, C-645/19 (  
Facebook Ireland and Others  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Competence   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Tasks   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Powers   
General data protection law   
 >   
Chapter VII - Cooperation and consistency   
 >   
Cooperation   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Powers   
   
JUDGMENT OF THE COURT (Grand Chamber)  
15 June 2021 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 47 – Regulation (EU) 2016/679 – Cross-border processing of personal data – ‘One-stop shop’ mechanism – Sincere and effective cooperation between supervisory authorities – Competences and powers – Power to initiate or engage in legal proceedings)  
In Case C-645/19,  
REQUEST for a preliminary ruling under Article 267 TFEU from the hof van beroep te Brussel (Court of Appeal, Brussels, Belgium,), made by decision of 8 May 2019, received at the Court on 30 August 2019, in the proceedings  
Facebook Ireland Ltd,  
Facebook Inc.,  
Facebook Belgium BVBA,  
v  
Gegevensbeschermingsautoriteit,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, A. Arabadjiev, A. Prechal, M. Vilaras, M. Ilešič and N. Wahl, Presidents of Chambers, E. Juhász, D. Šváby, S. Rodin, F. Biltgen, K. Jürimäe, C. Lycourgos, P.G. Xuereb and L.S. Rossi (Rapporteur), Judges,  
Advocate General: M. Bobek,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 5 October 2020,  
after considering the observations submitted on behalf of:  
–        Facebook Ireland Ltd, Facebook Inc. and Facebook Belgium BVBA, by S. Raes, P. Lefebvre and D. Van Liedekerke, advocaten,  
–        the Gegevensbeschermingsautoriteit, by F. Debusseré and R. Roex, avocaten,  
–        the Belgian Government, by J.-C. Halleux, P. Cottin, and C. Pochet, acting as Agents, and by P. Paepe, advocaat,  
–        the Czech Government, by M. Smolek, O. Serdula and J. Vláčil, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by G. Natale, avvocato dello Stato,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes, A.C. Guerra, P. Barros da Costa and L. Medeiros, acting as Agents,  
–        the Finnish Government, by A. Laine and M. Pere, acting as Agents,  
–        the European Commission, by H. Kranenborg, D. Nardi and P.J.O. Van Nuffel, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 13 January 2021,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 55(1), Articles 56 to 58 and Articles 60 to 66 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2), read together with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between Facebook Ireland Ltd, Facebook Inc. and Facebook Belgium BVBA, on the one hand, and the Gegevensbeschermingsautoriteit (the Belgian Data Protection Authority) (‘the DPA’), as the successor of the Commissie ter bescherming van de Persoonlijke Levenssfeer (the Belgian Privacy Commission) (‘the Privacy Commission’), on the other, concerning injunction proceedings brought by the President of the Privacy Commission seeking to bring to an end the processing of personal data, of internet users within Belgium, by the Facebook online social network, using cookies, social plug-ins and pixels.  
   
Legal context  
   
European Union law  
3        Recitals 1, 4, 10, 11, 13, 22, 123, 141 and 145 of Regulation 2016/679 state:  
‘(1)      The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the [Charter] and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.  
…  
(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.  
…  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
(11)      Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.  
…  
(13)      In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States.  
…  
(22)      Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.  
…  
(123)      The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the [European] Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.  
…  
(141)      Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. …  
…  
(145)      For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.’  
4        Article 3(1) of that regulation, that article being headed ‘Territorial scope’, provides:  
‘This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.’  
5        Article 4 of that regulation defines, in point (16), the concept of ‘main establishment’ and, in point (23), the concept of ‘cross-border processing’ as follows:  
‘(16)      “main establishment” means:  
(a)      as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;  
(b)      as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;  
…  
(23)      “cross-border processing” means either:  
(a)      processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or  
(b)      processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.’  
6        Article 51 of that regulation, headed ‘Supervisory authority’, provides:  
‘1.      Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union …  
2.      Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.  
…’  
7        Article 55 of Regulation 2016/679, headed ‘Competence’, which forms part of Chapter VI of that regulation, entitled ‘Independent supervisory authorities’, provides:  
‘1.      Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.  
2.      Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.’  
8        Article 56 of that regulation, headed ‘Competence of the lead supervisory authority’, states:  
‘1.      Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.  
2.      By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.  
3.      In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.  
4.      Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).  
5.      Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.  
6.      The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.’  
9        Article 57(1) of Regulation 2016/679, that article being headed ‘Tasks’, provides:  
‘1.      Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:  
(a)      monitor and enforce the application of this Regulation;  
…  
(g)      cooperate with, including sharing information, and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;  
…’  
10      Article 58(1), (4) and (5) of that regulation, that article being headed ‘Powers’, provide:  
‘1.      Each supervisory authority shall have all of the following investigative powers:  
(a)      to order the controller and the processor, and, where applicable, the controller’s or the processor’s representative to provide any information it requires for the performance of its tasks;  
…  
(d)      to notify the controller or the processor of an alleged infringement of this Regulation;  
…  
4.      The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in [EU law] and Member State law in accordance with the Charter.  
5.      Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to initiate or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.’  
11      Within Chapter VII of Regulation 2016/679, entitled ‘Cooperation and consistency’, Section I, entitled ‘Cooperation’, contains Articles 60 to 62 of that regulation. Article 60, headed ‘Cooperation between the lead supervisory authority and the other supervisory authorities concerned’, provides:  
‘1.      The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.  
2.      The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.  
3.      The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.  
4.      Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.  
5.      Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.  
6.      Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.  
7.      The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be, and inform the other supervisory authorities concerned and the [European Data Protection] Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.  
8.      By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.  
9.      Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. …  
10.      After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.  
11.      Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.  
…’  
12      Article 61(1) of that regulation, that article being headed ‘Mutual assistance’, states:  
‘Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.’  
13      Article 62 of that regulation, headed ‘Joint operations of supervisory authorities’, provides:  
‘1.      The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.  
2.      Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. …  
…’  
14      Section 2, entitled ‘Consistency’, of Chapter VII of Regulation 2016/679 contains Articles 63 to 67 of that regulation. Article 63, headed ‘Consistency mechanism’, is worded as follows:  
‘In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.’  
15      Article 64(2) of that regulation is worded as follows:  
‘Any supervisory authority, the Chair of the [European Data Protection] Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the [European Data Protection] Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.’  
16      Article 65(1) of that regulation, that article being headed ‘Dispute resolution by the Board’, provides:  
‘In order to ensure the correct and consistent application of this Regulation in individual cases, the [European Data Protection] Board shall adopt a binding decision in the following cases:  
(a)      where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;  
(b)      where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;  
…’  
17      Article 66(1) and (2) of Regulation 2016/679, that article being headed ‘Urgency procedure’, provide:  
‘1.      In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the [European Data Protection] Board and to the Commission.  
2.      Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the [European Data Protection] Board, giving reasons for requesting such opinion or decision.’  
18      Article 77 of that regulation, headed ‘Right to lodge a complaint with a supervisory authority’, states:  
‘1.      Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.  
2.      The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.’  
19      Article 78 of that regulation, headed ‘Right to an effective judicial remedy against a supervisory authority’, provides:  
‘1.      Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.  
2.      Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.  
3.      Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.  
4.      Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the [European Data Protection] Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.’  
20      Article 79 of that regulation, headed ‘Right to an effective judicial remedy against a controller or processor’, states:  
‘1.      Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.  
2.      Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.’  
   
National law  
21      The wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens (law on the protection of privacy with regard to the processing of personal data) of 8 December 1992 (  
Belgisch Staatsblad  
, 18 March 1993, p. 5801), as amended by the law of 11 December 1998 (  
Belgisch Staatsblad  
, 3 February 1999, p. 3049) (‘the law of 8 December 1992’), transposed into Belgian law Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
22      The law of 8 December 1992 established the Privacy Commission, an independent body responsible for ensuring that the processing of personal data should comply with that law, in order to protect citizens’ privacy.  
23      Article 32(3) of the Law of 8 December 1992 provided:  
‘Without prejudice to the jurisdiction of the ordinary courts and tribunals for the application of the general principles relating to the protection of privacy, the President of the [Privacy Commission] may bring before the court of first instance any dispute concerning the application of this legislation and its implementing measures.’  
24      The wet tot oprichting van de Gegevensbeschermingsautoriteit (law creating a data protection authority) of 3 December 2017 (  
Belgisch Staatsblad  
, 10 January 2018, p. 989; ‘the law of 3 December 2017’), which entered into force on 25 May 2018, established the DPA as a supervisory authority, within the meaning of Regulation 2016/679.  
25      Article 3 of the Law of 3 December 2017 provides:  
‘There shall be established at the Belgian Chamber of Representatives a “Data Protection Authority”. It shall succeed the [Privacy Commission].’  
26      Article 6 of the Law of 3 December 2017 provides:  
‘The [DPA] has the power to bring any infringement of the fundamental principles of personal data protection, within the framework of this law and laws containing provisions on the protection of the processing of personal data, to the attention of the judicial authorities and, where appropriate, to initiate or engage in legal proceedings to have these fundamental principles applied.’  
27      There is no specific provision in relation to court proceedings already commenced by the President of the Privacy Commission as at 25 May 2018 on the basis of Article 32(3) of the law of 8 December 1992. As regards solely complaints or applications lodged with the DPA itself, Article 112 of the law of 3 December 2017 states:  
‘Chapter VI shall not apply to complaints or applications still pending at the [DPA] at the time when this legislation enters into force. The complaints or applications mentioned in subparagraph 1 shall be dealt with by the [DPA], as the legal successor of the [Privacy Commission], in accordance with the procedure applicable before the entry into force of this legislation.’  
28      The law of 8 December 1992 was repealed by the wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (law on the protection of individuals with regard to the processing of personal data) of 30 July 2018 (  
Belgisch Staatsblad  
, 5 September 2018, p. 68616; ‘the law of 30 July 2018’). That law transposes into Belgian law the provisions of Regulation 2016/679 requiring or permitting Member States to adopt more detailed rules, to supplement that regulation.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
29      On 11 September 2015 the President of the Privacy Commission brought legal proceedings seeking an injunction against Facebook Ireland, Facebook Inc. and Facebook Belgium before the Nederlandstalige rechtbank van eerste aanleg Brussel (Dutch-language Court of First Instance, Brussels, Belgium). Since the Privacy Commission had no legal personality, it was necessary that the President of that body take legal action in order to ensure compliance with the legislation on the protection of personal data. However, the Privacy Commission itself sought leave to intervene in the proceedings brought by its President.  
30      The object of those injunction proceedings was to bring to an end what the Privacy Commission describes, inter alia, as a ‘serious and large-scale infringement, by Facebook, of the legislation relating to the protection of privacy’ consisting in the collection by that online social network of information on the internet browsing behaviour both of Facebook account holders and of non-users of Facebook services by means of various technologies, such as cookies, social plug-ins (for example, the ‘Like’ or ‘Share’ buttons) or pixels. Those features permit Facebook to obtain certain data of an internet user who visits a website page containing them, such as the address of that page, the ‘IP address’ of the visitor to that page and the date and time of the visit in question.   
31      By judgment of 16 February 2018, the Nederlandstalige rechtbank van eerste aanleg Brussel (Dutch-language Court of First Instance, Brussels) held that it had jurisdiction to give a ruling on those injunction proceedings, in so far as the action concerned Facebook Ireland, Facebook Inc. and Facebook Belgium, and declared that the application for leave to intervene made by the Privacy Commission was inadmissible.  
32      On the substance, that court held that Facebook was not adequately informing Belgian internet users of the collection of the information concerned and of the use of that information. Further, the consent given by the internet users to the collection and processing of that data was held to be invalid. Consequently, that court ordered Facebook Ireland, Facebook Inc. and Facebook Belgium (i) to desist, as regards all internet users established in Belgium, from placing, without their consent, cookies that remain active for two years on the devices used by them when browsing a web page in the Facebook.com domain or visiting the website of a third party, and from placing cookies and collecting data by means of social plug-ins, pixels or similar technological means on third-party websites, in a manner that was excessive in the light of the objectives thereby pursued by the Facebook social network, (ii) to desist from providing information that might reasonably mislead the data subjects as to the real extent of the mechanisms put in place by Facebook for the use of cookies, and (iii) to destroy all the personal data obtained by means of cookies and social plug-ins.  
33      On 2 March 2018 Facebook Ireland, Facebook Inc. and Facebook Belgium brought an appeal against that judgment before the hof van beroep te Brussel (Court of Appeal, Brussels, Belgium). Before that court, the DPA acts as the legal successor both of the President of the Privacy Commission, who had brought the injunction proceedings, and of the Privacy Commission itself.  
34      The referring court held that it has jurisdiction solely to give a ruling on the appeal brought in so far as that appeal concerns Facebook Belgium. Conversely, the referring court held that it lacked jurisdiction to hear that appeal in relation to Facebook Ireland and Facebook Inc.  
35      Before giving a ruling on the substance of the main proceedings, a question raised by the referring court is whether the DPA had the required standing and interest to bring proceedings. In the view of Facebook Belgium, the action brought seeking an injunction is inadmissible, in so far as it concerns facts prior to 25 May 2018, given that, following the entry into force of the law of 3 December 2017 and of Regulation 2016/679, Article 32(3) of the law of 8 December 1992, which is the legal basis for bringing such an action, was repealed. As regards the facts subsequent to 25 May 2018, Facebook Belgium claims that the DPA has no competence and has no right to bring such an action given the existence of the ‘one-stop shop’ mechanism now provided for under the provisions of Regulation 2016/679. On the basis of those provisions, it is claimed that only the Data Protection Commissioner (Ireland) is competent to bring injunction proceedings against Facebook Ireland, the latter being the sole controller of the personal data of the users of the social network concerned within the European Union.  
36      The referring court has held that the DPA had not demonstrated the required standing to bring the injunction proceedings in so far as those proceedings related to facts prior to 25 May 2018. As regards the facts subsequent to that date, the referring court is however uncertain as to the effect of the entry into force of Regulation 2016/679, in particular the effect of the application of the ‘one-stop shop’ mechanism provided for by that regulation, on the competences of the DPA and on its power to bring such injunction proceedings.  
37      In particular, in the view of the referring court, the question that now arises is whether, with respect to the facts subsequent to 25 May 2018, the DPA may bring an action against Facebook Belgium, since Facebook Ireland has been identified as the controller of the data concerned. Since that date and by virtue of the ‘one-stop shop’ rule, it appears that, in accordance with Article 56 of Regulation 2016/679, only the Data Protection Commissioner (Ireland) is competent, subject to review only by the Irish courts.  
38      The referring court recalls that, in the judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
 (C-210/16, EU:C:2018:388), the Court held that the ‘German supervisory authority’ was competent in respect of data processing where the controller of the data concerned was established in Ireland and the subsidiary that was established in Germany (namely Facebook Germany GmbH) was responsible solely for the sale of advertising spots and other marketing activities in Germany.  
39      However, in the case that gave rise to that judgment, the Court was required to give a ruling on a request for a preliminary ruling concerning the interpretation of the provisions of Directive 95/46, which has been repealed by Regulation 2016/679. The referring court is uncertain to what extent the Court’s interpretation in that judgment is still of relevance to the application of Regulation 2016/679.  
40      The referring court also mentions a decision of the Bundeskartellamt (the German competition authority) of 6 February 2019 (the so-called ‘Facebook’ decision), in which that competition authority took the view that Facebook was abusing its position by merging data from different sources, which is now permitted only if users have given their explicit consent, with the proviso that any user who does not give his or her consent may not be excluded from Facebook services. The referring court notes that the Bundeskartellamt clearly considered itself to be competent, in spite of the ‘one-stop shop’ mechanism.  
41      Further, the referring court considers that Article 6 of the law of 3 December 2017, which permits, as a general rule, the DPA, where necessary, to initiate or to engage in legal proceedings, does not imply that the action may, in all circumstances, be brought by the DPA before the Belgian courts, since the ‘one-stop shop’ mechanism appears to require that such an action should be brought before the court with jurisdiction in the place where the data processing is carried out.  
42      In those circumstances, the hof van beroep te Brussel (Court of Appeal, Brussels) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Should Article 55(1), Articles 56 to 58 and Articles 60 to 66 of [Regulation 2016/679], read together with Articles 7, 8 and 47 of the [Charter], be interpreted as meaning that a supervisory authority which, pursuant to national law adopted in implementation of Article 58(5) of that regulation, has the competence to initiate or engage in legal proceedings before a court in its Member State against infringements of that regulation cannot exercise that competence in connection with cross-border data processing if it is not the lead supervisory authority for that cross-border data processing?  
(2)      Does the answer to the first question referred differ if the controller of that cross-border data processing does not have its main establishment in that Member State but does have another establishment there?  
(3)      Does the answer to the first question referred differ if the national supervisory authority initiates the legal proceedings against the main establishment of the controller in respect of the cross-border data processing rather than against the establishment in its own Member State?  
(4)      Does the answer to the first question referred differ if the national supervisory authority had already initiated the legal proceedings before the date on which [Regulation 2016/679] entered into force (25 May 2018)?  
(5)      If the first question referred is answered in the affirmative, does Article 58(5) of [Regulation 2016/679] have direct effect, meaning that a national supervisory authority can rely on that provision to initiate or continue legal proceedings against private parties even if Article 58(5) of [Regulation 2016/679] has not been specifically transposed into the legislation of the Member States, notwithstanding the requirement to do so?  
(6)      If questions (1) to (5) are answered in the affirmative, could the outcome of such proceedings prevent the lead supervisory authority from making a contrary finding when the lead supervisory authority investigates the same or similar cross-border processing activities in accordance with the mechanism laid down in Articles 56 and 60 of [Regulation 2016/679]?’  
   
 Consideration of the questions referred  
   
The first question  
43      By its first question, the referring court seeks, in essence, to ascertain whether Article 55(1), Articles 56 to 58 and Articles 60 to 66 of Regulation 2016/679, read together with Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a supervisory authority of a Member State which, under the national legislation adopted in order to implement Article 58(5) of that regulation, has the power to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where necessary, to initiate or engage in legal proceedings, may exercise that power with respect to cross-border data processing even though it is not the ‘lead supervisory authority’, within the meaning of Article 56(1) of that regulation, in relation to such data processing.  
44      In that regard, it must recalled, as a preliminary point, that, first, unlike Directive 95/46, which had been adopted on the basis of Article 100 A of the EC Treaty, concerning the harmonisation of the common market, the legal basis of Regulation 2016/679 is Article 16 TFEU, which enshrines the right of everyone to the protection of personal data concerning them and authorises the European Parliament and the Council of the European Union to lay down the rules relating to the protection of individuals with regard to the processing of that data by European Union institutions, bodies, offices and agencies, and by the Member States, when carrying out activities which fall within the scope of EU law, and the rules relating to the free movement of such data. Second, recital 1 of that regulation confirms that ‘the protection of natural persons in relation to the processing of personal data is a fundamental right’ and states that Article 8(1) of the Charter and Article 16(1) TFEU lay down the right of everyone to the protection of personal data concerning them.  
45      Consequently, as is clear from its Article 1(2), read together with recitals 10, 11 and 13 thereof, Regulation 2016/679 requires the European Union institutions, bodies, offices and agencies, and the competent authorities of the Member States, to ensure a high level of protection of the rights guaranteed in Article 16 TFEU and Article 8 of the Charter.  
46      Further, as stated in its recital 4, Regulation 2016/679 respects all fundamental rights and observes the freedoms and principles recognised in the Charter.  
47      Against that background, Article 55(1) of Regulation 2016/679 states the general rule that each supervisory authority is to be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it, in accordance with that regulation, on the territory of its own Member State (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 147).  
48      One of the tasks assigned to those supervisory authorities is the task of monitoring the application of Regulation 2016/679 and enforcing its application, as laid down in Article 57(1)(a) of that regulation, while another is the task of cooperating with other supervisory authorities, including sharing information, and providing mutual assistance with a view to ensuring the consistency of application and enforcement of that regulation, as laid down in Article 57(1)(g) of that regulation. The powers conferred on those supervisory authorities, for the performance of those tasks, include various investigative powers, laid down in Article 58(1) of Regulation 2016/679, and the power to bring any infringement of that regulation to the attention of the judicial authorities and, where appropriate, to initiate or engage in legal proceedings in order to enforce the provisions of that regulation, as laid down in Article 58(5) of that regulation.   
49      The performance of those tasks and the exercise of those powers presupposes, however, that a supervisory authority is competent with respect to a particular instance of data processing.  
50      In that regard, without prejudice to the rule on competence set out in Article 55(1) of Regulation 2016/679, Article 56(1) of that regulation establishes, with respect to ‘cross-border processing’, within the meaning of Article 4, point (23), of that regulation, the ‘one-stop shop’ mechanism, based on an allocation of competences between one ‘lead supervisory authority’ and the other supervisory authorities concerned. Under that mechanism, the supervisory authority of the main establishment or of the single establishment of the controller or processor is to be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor, in accordance with the procedure set out in Article 60 of that regulation.  
51      Article 60 establishes the procedure for cooperation between the lead supervisory authority and the other supervisory authorities concerned. As part of that procedure, the lead supervisory authority is, in particular, required to endeavour to reach consensus. To that end, in accordance with Article 60(3) of Regulation 2016/679, the lead supervisory authority is without delay to submit a draft decision to the other supervisory authorities concerned for their opinion and is to take due account of their views.   
52      It follows more specifically from Articles 56 and 60 of Regulation 2016/679 that, with respect to ‘cross-border processing’, within the meaning of Article 4, point (23), of that regulation, and subject to Article 56(2) thereof, the various national supervisory authorities concerned must cooperate, in accordance with the procedure laid down in those provisions, in order to reach a consensus and a single decision, which is binding on all those authorities and with which decision the controller must ensure compliance as regards processing activities undertaken in the context of all its establishments within the European Union. Further, Article 61(1) of that regulation obliges the supervisory authorities, inter alia, to provide each other with relevant information and mutual assistance in order to implement and apply that regulation in a consistent manner throughout the European Union. Article 63 of Regulation 2016/679 states that it was for that purpose that provision was made for the consistency mechanism, set out in Articles 64 and 65 of that regulation (judgment of 24 September 2019,   
Google   
(Territorial scope of de  
-  
referencing)  
, C-507/17, EU:C:2019:772, paragraph 68).  
53      The application of the ‘one-stop shop’ mechanism consequently requires, as confirmed in recital 13 of Regulation 2016/679, sincere and effective cooperation between the lead supervisory authority and the other supervisory authorities concerned. Accordingly, as the Advocate General stated in point 111 of his Opinion, the lead supervisory authority may not ignore the views of the other supervisory authorities, and any relevant and reasoned objection made by one of the other supervisory authorities has the effect of blocking, at least temporarily, the adoption of the draft decision of the lead supervisory authority.  
54      Thus, in accordance with Article 60(4) of Regulation 2016/679, where one of the other supervisory authorities concerned expresses, within a period of four weeks after having been consulted, such a relevant and reasoned objection to the draft decision, the lead supervisory authority, if it does not follow the relevant and reasoned objection or is of the opinion that that objection is not relevant or reasoned, is to submit the matter to the consistency mechanism provided for in Article 63 of that regulation, in order to obtain a binding decision, adopted on the basis of Article 65(1)(a) of that regulation, from the European Data Protection Board.  
55      Under Article 60(5) of Regulation 2016/679, where the lead supervisory authority intends, on the other hand, to follow the relevant and reasoned objection made, it must submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision is to be subject to the procedure referred to in Article 60(4) within a period of two weeks.  
56      In accordance with Article 60(7) of that regulation, it is the responsibility of the lead supervisory authority, as a general rule, to adopt a decision with respect to the cross-border processing concerned, to give notice of that decision to the main establishment or the single establishment of the controller or processor, as the case may be, and to inform the other supervisory authorities concerned and the European Data Protection Board of the decision in question, including a summary of the relevant facts and grounds.  
57      That said, it must be noted that Regulation 2016/679 establishes exceptions to the general rule that it is the lead supervisory authority which is competent to adopt decisions in the context of the ‘one-stop shop’ mechanism provided for in Article 56(1) of that regulation.  
58      The first of those exceptions is to be found in Article 56(2) of Regulation 2016/679, which provides that a supervisory authority which is not the lead supervisory authority is to be competent to handle a complaint lodged with it concerning a cross-border processing of personal data or a possible infringement of that regulation, if the subject matter relates only to an establishment in its own Member State or substantially affects data subjects only in that Member State.  
59      The second exception is in Article 66 of Regulation 2016/679, which provides, by way of derogation from the consistency mechanisms referred to in Articles 60 and Article 63 to 65 of that regulation, for an urgency procedure. That urgency procedure makes it possible, in exceptional circumstances, where the supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, immediately to adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which is not to exceed three months, while Article 66(2) of Regulation 2016/679 further provides that, where a supervisory authority has taken a measure under Article 66(1) and considers that final measures must urgently be adopted, it may request an urgent opinion or an urgent binding decision from the European Data Protection Board, giving reasons for requesting such an opinion or decision.  
60      However, the exercise of that competence by the supervisory authorities must be compatible with the need for sincere and effective cooperation with the lead supervisory authority, in accordance with the procedure referred to in Article 56(3) to (5) of Regulation 2016/679. In such circumstances, under Article 56(3) of that regulation, the supervisory authority concerned must without delay inform the lead supervisory authority, which, within a period of three weeks of being informed, is to decide whether or not it will handle the case.  
61      Under Article 56(4) of Regulation 2016/679, where the lead supervisory authority decides to handle the case, the cooperation procedure laid down in Article 60 of that regulation is applicable. In that context, the supervisory authority which informed the lead supervisory authority may submit to the latter a draft for a decision and the latter must take the utmost account of that draft when preparing the draft decision referred to in Article 60(3) of that regulation.  
62      However, under Article 56(5) of Regulation 2016/679, where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the former is to handle the case in accordance with Articles 61 and 62 of that regulation, those provisions requiring the supervisory authorities to comply with the rules on mutual assistance and cooperation within the framework of joint operations, in order to ensure effective cooperation between the authorities concerned.  
63      It follows from the foregoing that, first, in relation to the cross-border processing of personal data, the competence of the lead supervisory authority for the adoption of a decision finding that such processing is an infringement of the rules relating to the protection of the rights of natural persons as regards the processing of personal data found in Regulation 2016/679 constitutes the rule, whereas the competence of the other supervisory authorities concerned for the adoption of such a decision, even provisionally, constitutes the exception. Second, while the competence as a general rule of the lead supervisory authority is confirmed in Article 56(6) of Regulation 2016/679, which states that the lead supervisory authority is the ‘sole interlocutor’ of the controller or processor with respect to the cross-border processing carried out by that controller or that processor, that authority must exercise such competence within a framework of close cooperation with the other supervisory authorities concerned. In particular, the lead supervisory authority cannot, in the exercise of its competences, as stated in paragraph 53 of the present judgment, eschew essential dialogue with and sincere and effective cooperation with the other supervisory authorities concerned.   
64      In that regard, it is stated in recital 10 of Regulation 2016/679 that that regulation seeks, inter alia, to ensure consistent and homogeneous application of the rules for the protection of the freedoms and fundamental rights of natural persons with regard to the processing of personal data throughout the European Union and to remove obstacles to flows of personal data within the Union.   
65      That objective, and the effectiveness of the ‘one-stop shop’ mechanism, might be jeopardised if a supervisory authority which is not, with respect to an instance of cross-border data processing, the lead supervisory authority, could exercise the power laid down in Article 58(5) of Regulation 2016/679 in situations other than those where it has competence for the adoption of a decision as referred to in paragraph 63 of the present judgment. The exercise of that power is indeed intended to lead to a binding judicial decision, which is no less liable to undermine that objective and that mechanism than a decision adopted by a supervisory authority which is not the lead supervisory authority.  
66      Contrary to what is claimed by the DPA, the fact that a supervisory authority of a Member State which is not the lead supervisory authority may exercise the power laid down in Article 58(5) of Regulation 2016/679 only when that exercise complies with the rules on the allocation of competences to adopt decisions laid down, in particular, in Articles 55 and 56 of that regulation, read together with Article 60 thereof, is compatible with Articles 7, 8 and 47 of the Charter.   
67      First, as regards the argument concerning an alleged breach of Articles 7 and 8 of the Charter, it must be recalled that Article 7 guarantees that everyone has the right to respect for his or her private and family life, home and communications, whereas Article 8(1) of the Charter, like Article 16(1) TFEU, expressly recognises that everyone has the right to the protection of personal data concerning him or her. It is clear, in particular, from Article 51(1) of Regulation 2016/679 that the supervisory authorities are responsible for monitoring the application of that regulation, for the purpose, inter alia, of protecting the fundamental rights of natural persons as regards the processing of their personal data. It follows that, in line with what has been said in paragraph 45 of the present judgment, the rules on the allocation of competences to adopt decisions between the lead supervisory authority and the other supervisory authorities, as laid down by that regulation, take nothing away from the responsibility incumbent on each of those authorities to contribute to a high level of protection of those rights, with due regard to those rules and to the requirements of cooperation and mutual assistance mentioned in paragraph 52 of the present judgment.   
68      That means, in particular, that the use of the ‘one-stop shop’ mechanism cannot under any circumstances have the consequence that a national supervisory authority, in particular the lead supervisory authority, does not assume the responsibility incumbent on it under Regulation 2016/679 to contribute to providing effective protection of natural persons from infringements of their fundamental rights as recalled in the preceding paragraph of the present judgment, as otherwise that consequence might encourage the practice of   
forum shopping  
, particularly by data controllers, designed to circumvent those fundamental rights and the practical application of the provisions of that regulation that give effect to those rights.   
69      Second, as regards the argument concerning the alleged breach of the right to an effective remedy, guaranteed in Article 47 of the Charter, that argument cannot be accepted either. The manner in which, as set out in paragraphs 64 and 65 of the present judgment, the possibility that a supervisory authority other than the lead supervisory authority may exercise the power laid down in Article 58(5) of Regulation 2016/679, with respect to an instance of cross-border processing of personal data, is circumscribed takes nothing away from the right of every data subject, laid down in Article 78(1) and (2) of that regulation, to an effective legal remedy, in particular, against a legally binding decision of a supervisory authority concerning him or her, or against a failure by the supervisory authority which has the competence to adopt decisions under Articles 55 and 56 of that regulation, read together with Article 60 thereof, to handle a complaint that that data subject has lodged.  
70      That is particularly true in the situation described in Article 56(5) of Regulation 2016/679, by virtue of which, as stated in paragraph 62 of the present judgment, the supervisory authority which has given information on the basis of Article 56(3) of that regulation, may handle the case in accordance with Articles 61 and 62 thereof, where the lead supervisory authority decides, after having been so informed, that it will not itself handle the case. If a case is to be handled in such a way, it is not inconceivable that the supervisory authority concerned may, where appropriate, decide to exercise the power conferred on it by Article 58(5) of Regulation 2016/679.  
71      That said, it must be emphasised that the exercise of the power of a Member State’s supervisory authority to bring actions before the courts of that State cannot be ruled out where, after the mutual assistance of the lead supervisory authority has been sought, under Article 61 of Regulation 2016/679, the latter does not provide the former with the requested information. In that situation, under Article 61(8) of that regulation, the supervisory authority concerned may adopt a provisional measure on the territory of its own Member State and, if it considers that there is an urgent need for the adoption of final measures, that authority may, in accordance with Article 66(2) of that regulation, request an urgent opinion or an urgent binding decision from the European Data Protection Board. Further, under Article 64(2) of that regulation, a supervisory authority may request that any matter that is of general application or that produces effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance imposed on it by Article 61 of that regulation. Following the adoption of such an opinion or such a decision, and provided that the European Data Protection Board approves, after taking account of all the relevant circumstances, the supervisory authority concerned must be able to take the necessary measures to ensure compliance with the rules on the protection of the rights of natural persons as regards the processing of personal data contained in Regulation 2016/679 and, for that purpose, exercise the power conferred on it by Article 58(5) of that regulation.  
72      The sharing of competences and responsibilities among the supervisory authorities is of necessity underpinned by the existence of sincere and effective cooperation, between those authorities and with the Commission, in order to ensure the correct and consistent application of that regulation, as Article 51(2) of that regulation confirms.  
73      In this instance, it will be for the referring court to determine whether the rules on the allocation of competences and the relevant procedures and mechanisms laid down by Regulation 2016/679 have been correctly applied in the main proceedings. In particular, it will be the task of the referring court to ascertain whether, although the DPA is not the lead supervisory authority in this case, the processing in question, to the extent that it involves the conduct of the Facebook online social network subsequent to 25 May 2018, may be classified as occurring in, in particular, the situation referred to in paragraph 71 of the present judgment.  
74      In that regard, the Court observes that the European Data Protection Board, in its Opinion 5/2019 of 12 March 2019 on the interplay between the [Directive on privacy and electronic communications] and the [General Data Protection Regulation], in particular regarding the competence, tasks and powers of data protection authorities, stated that storing and obtaining access to personal data by means of cookies fell within the scope of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), and not within the scope of the ‘one-stop shop’ mechanism. On the other hand, all earlier processing operations, and all subsequent processing activities, with respect to that personal data, by means of other technologies, do fall within the scope of Regulation 2016/679, and consequently within the scope of the ‘one-stop shop’ mechanism. Given that its request for mutual assistance concerned subsequent personal data processing operations, the DPA in April 2019 asked the Data Protection Commissioner (Ireland) to respond to its request as expeditiously as possible, but no response was provided.  
75      In the light of all the foregoing, the answer to the first question referred is that Article 55(1), Articles 56 to 58 and Articles 60 to 66 of Regulation 2016/679, read together with Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a supervisory authority of a Member State which, under the national legislation adopted in order to transpose Article 58(5) of that regulation, has the power to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where necessary, to initiate or engage in legal proceedings, may exercise that power in relation to an instance of cross-border data processing even though it is not the ‘lead supervisory authority’, within the meaning of Article 56(1) of that regulation, with respect to that data processing, provided that that power is exercised in one of the situations where that regulation confers on that supervisory authority a competence to adopt a decision finding that such processing is in breach of the rules contained in that regulation, and that the cooperation and consistency procedures laid down by that regulation are respected.  
   
The second question  
76      By its second question, the referring court seeks, in essence, to ascertain whether Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, in the event of cross-border data processing, it is a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings, within the meaning of that provision, that the controller with respect to the cross-border processing of personal data against whom such proceedings are brought has a ‘main establishment’, within the meaning of Article 4, point 16, of Regulation 2016/679, on the territory of that Member State or another establishment on that territory.  
77      In that regard, it must be recalled that, under Article 55(1) of Regulation 2016/679, each supervisory authority is to be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it, in accordance with that regulation, on the territory of its own Member State.   
78      Article 58(5) of Regulation 2016/679 lays down, further, the power of each supervisory authority to bring any alleged infringement of that regulation to the attention of a court of its Member State and, where appropriate, to initiate or engage in legal proceedings, in order to enforce the provisions of that regulation.  
79      It must be observed that Article 58(5) of Regulation 2016/679 is worded in general terms and that the EU legislature has not specified that the exercise of that power by a Member State’s supervisory authority is subject to the condition that its legal action should be brought against a controller who has a ‘main establishment’, within the meaning of Article 4, point 16, of that regulation, or another establishment on the territory of that Member State.  
80      However, a Member State’s supervisory authority may exercise the power conferred on it by Article 58(5) of Regulation 2016/679 only if it is demonstrated that that power falls within the territorial scope of that regulation.  
81      Article 3(1) of Regulation 2016/679, which governs the territorial scope of that regulation, provides, in that regard, that the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, whether or not the processing takes place in the European Union.  
82      In that connection, recital 22 of Regulation 2016/679 states that the existence of such an establishment implies the effective and real exercise of activity through stable arrangements and that the legal form of such arrangements, whether through a branch or a subsidiary with legal personality, is not the determining factor in that respect.  
83      It follows that, in accordance with Article 3(1) of Regulation 2016/679, the territorial scope of that regulation is determined, without prejudice to the situations referred to in paragraphs 2 and 3 of that article, by the condition that the controller or the processor with respect to the cross-border processing has an establishment in the European Union.  
84      Consequently the answer to the second question referred is that Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, in the event of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings, within the meaning of that provision, that the controller with respect to the cross-border processing of personal data against whom such proceedings are brought has a main establishment or another establishment on the territory of that Member State.  
   
The third question  
85      By its third question, the referring court seeks, in essence, to ascertain whether Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, in the event of cross-border data processing, it is a prerequisite of the exercise by a supervisory authority of a Member State, other than the lead supervisory authority, of the power to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where appropriate, to initiate or engage in legal proceedings, within the meaning of that provision, that the supervisory authority concerned directs its legal proceedings against the main establishment of the controller or against the establishment that is located in its own Member State.  
86      It is clear from the order for reference that that question has arisen in the context of argument by the parties in relation to the issue whether the referring court has jurisdiction to hear the injunction proceedings in so far as those proceedings are brought against Facebook Belgium, given that, first, within the European Union, the headquarters of the Facebook group is situated in Ireland and that Facebook Ireland is the sole controller with respect to the collection and processing of personal data throughout the European Union, and, second, due to the internal division of that group, the establishment located in Belgium was created, primarily, to allow the Facebook group to engage with the EU institutions and, secondarily, to promote the advertising and marketing of that group to people residing in Belgium.  
87      As stated in paragraph 47 of the present judgment, Article 55(1) of Regulation 2016/679 establishes the competence, as a general rule, of each supervisory authority for the performance of the tasks assigned to it and the exercise of the powers conferred on it, in accordance with that regulation, on the territory of its own Member State.  
88      As regards the power of a supervisory authority of a Member State to bring legal proceedings, within the meaning of Article 58(5) of Regulation 2016/679, it must be recalled, as the Advocate General stated in point 150 of his Opinion, that that provision is worded in general terms and that it does not specify against which entities the supervisory authorities should or might direct legal proceedings in relation to any infringement of that regulation.  
89      Consequently, that provision does not restrict the exercise of the power to initiate or engage in legal proceedings in such a way that those proceedings can solely be brought against a ‘main establishment’ or against some other ‘establishment’ of the controller. On the contrary, under Article 58(5) of that regulation, where the supervisory authority of a Member State has the necessary competence for that purpose, under Articles 55 and 56 of Regulation 2016/679, it may exercise the powers conferred by that regulation on its national territory, irrespective of the Member State in which the controller or its processor is established.  
90      However, the exercise of the power conferred on each supervisory authority in Article 58(5) of Regulation 2016/679 presupposes that that regulation is applicable. In that regard, and as stated in paragraph 81 of the present judgment, Article 3(1) of that regulation provides that it is applicable to the processing of personal data ‘in the context of the activities of an establishment of a controller or a processor in the [European] Union, whether or not the processing takes place in the [European] Union’.  
91      Having regard to the objective pursued by Regulation 2016/679, which is to ensure effective protection of the freedoms and fundamental rights of individuals, in particular, their right to protection of privacy and the protection of personal data, the condition that the processing of personal data must be carried out ‘in the context of the activities’ of the establishment concerned, cannot be interpreted restrictively (see, by analogy, judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig  
-  
Holstein  
, C-210/16, EU:C:2018:388, paragraph 56 and the case-law cited).  
92      In this instance, it is clear from the order for reference and from the written observations lodged by Facebook Belgium that the function of that company is, primarily, to engage with the EU institutions and, secondarily, to promote the advertising and marketing of the Facebook group aimed at people residing in Belgium.  
93      The objective of the processing of personal data at issue in the main proceedings, which is carried out within the European Union exclusively by Facebook Ireland and which consists in the collection of information on the internet browsing behaviour both of Facebook account holders and of non-users of Facebook services by means of various technologies, such as, inter alia, social plug-ins and pixels, is precisely to enable the social network concerned to make its advertising system more efficient by disseminating targeted communications.  
94      It must be observed that, first, a social network such as Facebook generates a substantial proportion of its income from, inter alia, the advertising that is disseminated on that social network, and that the activity carried out by the establishment located in Belgium is intended to ensure, within Belgium, even if it is only a secondary function, the promotion and sale of advertising spots which serve to make Facebook services profitable. Second, the activity primarily carried out by Facebook Belgium, which consists in engaging with the EU institutions and constituting a point of contact for those institutions, seeks, inter alia, to determine the personal data processing policy of Facebook Ireland.  
95      In those circumstances, the activities of the establishment of the Facebook group located in Belgium must be considered to be inextricably linked to the processing of personal data at issue in the main proceedings, with respect to which Facebook Ireland is the controller within the European Union. Accordingly, that processing must be regarded as being carried out ‘in the context of the activities of an establishment of a controller’, within the meaning of Article 3(1) of Regulation 2016/679.  
96      In the light of all the foregoing, the answer to the third question referred is that Article 58(5) of Regulation 2016/679 must be interpreted as meaning that the power of a supervisory authority of a Member State, other than the lead supervisory authority, to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where appropriate, to initiate or engage in legal proceedings, within the meaning of that provision, may be exercised both with respect to the main establishment of the controller which is located in that authority’s own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power, in accordance with the terms of the answer to the first question referred.   
   
The fourth question  
97      By its fourth question, the referring court seeks, in essence, to ascertain whether Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, where a supervisory authority of a Member State which is not the ‘lead supervisory authority’, within the meaning of Article 56(1) of that regulation, has before 25 May 2018 brought legal proceedings concerning an instance of cross-border processing of personal data, that is, before the date when that regulation became applicable, that fact is such as to affect the conditions governing whether a Member State’s supervisory authority may exercise the power to initiate or engage in legal proceedings conferred on it by Article 58(5).  
98      The claim made before that court by Facebook Ireland, Facebook Inc. and Facebook Belgium is that the consequence of Regulation 2016/679 becoming applicable after 25 May 2018 is that the continuation of an action brought before that date is inadmissible, or unfounded.  
99      It must be noted, first, that Article 99(1) of Regulation 2016/679 provides that that regulation is to enter into force on the twentieth day following that of its publication in the   
Official   
Journal of the European Union  
. Since that regulation was published in the Official Journal on 4 May 2016, it therefore entered into force on 25 May 2016. Further, Article 99(2) of that regulation provides that it is to apply from 25 May 2018.  
100    In that regard, it should be borne in mind that a new rule of law applies from the entry into force of the act introducing it, and, while it does not apply to legal situations that have arisen and become definitive under the old law, it does apply to their future effects, and to new legal situations. It is otherwise, subject to the principle of the non-retroactivity of legal acts, only if the new rule is accompanied by special provisions which specifically lay down its conditions of temporal application. In particular, procedural rules are generally taken to apply from the date on which they enter into force, as opposed to substantive rules, which are usually interpreted as applying to situations existing before their entry into force only in so far as it follows clearly from their terms, their objectives or their general scheme that such an effect must be given to them (judgment of 25 February 2021,   
Caisse pour l’avenir des enfants   
(Employment at the time of birth)  
, C-129/20, EU:C:2021:140, paragraph 31 and the case-law cited).  
101    Regulation 2016/679 contains no transitional rule nor any other rule governing the status of court proceedings which were initiated before that regulation became applicable and which were still ongoing when it became applicable. In particular, there is no provision of that regulation which states that its effect is to bring to an end all court proceedings that are pending as at 25 May 2018 concerning alleged infringements of rules governing the processing of personal data laid down by Directive 95/46, even where the conduct that is a constituent element of such alleged infringements persists beyond that date.  
102    In this instance, Article 58(5) of Regulation 2016/679 lays down rules governing the power of a supervisory authority to bring any infringement of that regulation to the attention of the judicial authorities and, where appropriate, to initiate or engage otherwise in legal proceedings, in order to enforce the provisions of that regulation.  
103    In those circumstances, a distinction must be drawn between actions brought by a supervisory authority of a Member State with respect to infringements of the rules for the protection of personal data committed by controllers or processors before the date when Regulation 2016/679 became applicable and actions brought with respect to infringements committed after that date.  
104    In the first situation, from the perspective of EU law, a legal action, such as that at issue in the main proceedings, may be continued on the basis of the provisions of Directive 95/46, which remains applicable in relation to infringements committed up to the date of its repeal, namely 25 May 2018. In the second situation, such an action may be brought, under Article 58(5) of Regulation 2016/679, solely on the condition that, as was stated in the context of the answer to the first question referred, that action is brought in a situation where, exceptionally, that regulation confers on a supervisory authority of a Member State which is not the ‘lead supervisory authority’ a competence to adopt a decision finding that the processing of data in question is in breach of the rules contained in that regulation with respect to the protection of the rights of natural persons as regard the processing of personal data, with due regard to the procedures laid down by that regulation.  
105    In the light of all the foregoing, the answer to the fourth question referred is that Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, where a supervisory authority of a Member State which is not the ‘lead supervisory authority’, within the meaning of Article 56(1) of that regulation, has brought a legal action, the object of which is an instance of cross-border processing of personal data, before 25 May 2018, that is, before the date when that regulation became applicable, that action may, from the perspective of EU law, be continued on the basis of the provisions of Directive 95/46, which remains applicable in relation to infringements of the rules laid down in that directive committed up to the date when that directive was repealed. That action may, in addition, be brought by that authority with respect to infringements committed after that date, on the basis of Article 58(5) of Regulation 2016/679, provided that that action is brought in one of the situations where, exceptionally, that regulation confers on a supervisory authority of a Member State which is not the ‘lead supervisory authority’ a competence to adopt a decision finding that the processing of data in question is in breach of the rules contained in that regulation with respect to protection of the rights of natural persons as regard the processing of personal data, and that the cooperation and consistency procedures laid down by that regulation are respected, which it is for the referring court to determine.  
   
The fifth question  
106    By its fifth question, the referring court seeks, in essence, to ascertain whether, if the answer to the first question referred is in the affirmative, Article 58(5) of Regulation 2016/679 must be interpreted as meaning that that provision has direct effect, with the result that a national supervisory authority may rely on that provision in order to bring or continue a legal action against private parties, even where that provision has not been specifically implemented in the legislation of the Member State concerned.  
107    Article 58(5) of Regulation 2016/679 states that each Member State is to provide by law that its supervisory authority is to have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to initiate or engage otherwise in legal proceedings, in order to enforce the provisions of that regulation.  
108    First, it must be observed that, as submitted by the Belgian Government, Article 58(5) of Regulation 2016/679 has been implemented in the Belgian legal order by Article 6 of the law of 3 December 2017. Under that Article 6, the wording of which is essentially the same as that of Article 58(5) of Regulation 2016/679, the DPA has the power to bring any breach of the fundamental principles of the protection of personal data, in the context of that law and legislation containing provisions on the protection of processing of personal data, to the attention of the judicial authorities and, where appropriate, to initiate or engage in legal proceedings to enforce those fundamental principles. Consequently, it must be held that the DPA may rely on a provision of national law, such as Article 6 of the law of 3 December 2017, which implements Article 58(5) of Regulation 2016/679 in Belgian law, in order to initiate or engage in legal proceedings seeking to enforce that regulation.  
109    Further, for the sake of completeness, it must be observed that, under the second paragraph of Article 288 TFEU, a regulation is to be binding in its entirety and is to be directly applicable in all Member States, so that its provisions do not, as a general rule, require the adoption of any implementing measures by the Member States.  
110    In that regard, it must be recalled that, according to the Court’s settled case-law, pursuant to Article 288 TFEU and by virtue of the very nature of regulations and of their function in the system of sources of EU law, the provisions of those regulations generally have immediate effect in the national legal systems without its being necessary for the national authorities to adopt measures of application. Nonetheless, some of those provisions may necessitate, for their implementation, the adoption of measures of application by the Member States (judgment of 15 March 2017,   
Al Chodor  
, C-528/15, EU:C:2017:213, paragraph 27 and the case-law cited).  
111    However, as the Advocate General stated, in essence, in point 167 of his Opinion, Article 58(5) of Regulation 2016/679 lays down a specific and directly applicable rule which states that the supervisory authorities must have legal standing before the national courts and must have the power to initiate or engage in legal proceedings under national law.  
112    It is not stated in Article 58(5) of Regulation 2016/679 that Member States should determine by means of an express legal provision under what circumstances the national supervisory authorities may initiate or engage in legal proceedings, within the meaning of Article 58(5). It is sufficient that the supervisory authority should have the possibility, in accordance with national legislation, to bring to the attention of the judicial authorities infringements of that regulation and, where appropriate, to initiate or engage in legal proceedings or to commence, in some other manner, a procedure for the enforcement of the provisions of that regulation.  
113    In the light of all the foregoing, the answer to the fifth question referred is that Article 58(5) of Regulation 2016/679 must be interpreted as meaning that that provision has direct effect, with the result that a national supervisory authority may rely on that provision in order to bring or continue a legal action against private parties, even where that provision has not been specifically implemented in the legislation of the Member State concerned.  
   
The sixth question  
114    By its sixth question, the referring court seeks, in essence, to ascertain whether, in the event that the answer to the questions (1) to (5) referred is in the affirmative, the outcome of legal proceedings brought by a Member State’s supervisory authority in relation to an instance of cross-border processing of personal data may preclude the lead supervisory authority from adopting a decision in which it comes to the opposite conclusion where the latter authority investigates the same cross-border processing activities or similar activities, in accordance with the mechanism laid down in Articles 56 and 60 of Regulation 2016/679.  
115    In that regard, it should be borne in mind that, according to settled case-law, questions on the interpretation of EU law enjoy a presumption of relevance. The Court may refuse to give a ruling on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgments of 16 June 2015,   
Gauweiler and Others  
, C-62/14, EU:C:2015:400, paragraph 25, and of 7 February 2018,   
American Express  
, C-304/16, EU:C:2018:66, paragraph 32).  
116    Moreover, according to equally settled case-law, the justification for a reference for a preliminary ruling is not that it enables advisory opinions on general or hypothetical questions to be delivered but rather that it is necessary for the effective resolution of a dispute (judgment of 10 December 2018,   
Wightman and Others  
, C-621/18, EU:C:2018:999, paragraph 28 and the case-law cited).  
117    In this instance, it is clear that, as observed by the Belgian Government, the factual premiss of the sixth question referred has not been shown to have any reality in the context of the main proceedings, namely the premiss that, with respect to the cross-border processing that is the object of the dispute, there exists a lead supervisory authority which not only will investigate the same cross-border personal data processing activities as are the object of the legal proceedings initiated by the supervisory authority of the Member State concerned or similar activities, but, further, will contemplate the adoption of a decision that will reach the opposite conclusion.  
118    In those circumstances, it must be stated that the sixth question referred bears no relation to the actual facts of the main proceedings or their purpose, and concerns a hypothetical problem. Consequently, that question must be declared to be inadmissible.  
   
Costs  
119    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 55(1), Articles 56 to 58 and Articles 60 to 66 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), read together with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a supervisory authority of a Member State which, under the national legislation adopted in order to transpose Article 58(5) of that regulation, has the power to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where necessary, to initiate or engage in legal proceedings, may exercise that power in relation to an instance of cross  
-  
border data processing even though it is not the ‘lead supervisory authority’, within the meaning of Article 56(1) of that regulation, with respect to that data processing, provided that that power is exercised in one of the situations where Regulation 2016/679 confers on that supervisory authority a competence to adopt a decision finding that such processing is in breach of the rules contained in that regulation and that the cooperation and consistency procedures laid down by that regulation are respected.  
2.        
Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, in the event of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings, within the meaning of that provision, that the controller with respect to the cross-border processing of personal data against whom such proceedings are brought has a main establishment or another establishment on the territory of that Member State.  
3.        
Article 58(5) of Regulation 2016/679 must be interpreted as meaning that the power of a supervisory authority of a Member State, other than the lead supervisory authority, to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where appropriate, to initiate or engage in legal proceedings, within the meaning of that provision, may be exercised both with respect to the main establishment of the controller which is located in that authority’s own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power, in accordance with the terms of the answer to the first question referred.  
4.        
Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, where a supervisory authority of a Member State which is not the ‘lead supervisory authority’, within the meaning of Article 56(1) of that regulation, has brought a legal action, the object of which is an instance of cross-border processing of personal data, before 25 May 2018, that is, before the date when that regulation became applicable, that action may, from the perspective of EU law, be continued on the basis of the provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which remains applicable in relation to infringements of the rules laid down in that directive committed up to the date when that directive was repealed. That action may, in addition, be brought by that authority with respect to infringements committed after that date, on the basis of Article 58(5) of Regulation 2016/679, provided that that action is brought in one of the situations where, exceptionally, that regulation confers on a supervisory authority of a Member State which is not the ‘lead supervisory authority’ a competence to adopt a decision finding that the processing of data in question is in breach of the rules contained in that regulation with respect to the protection of the rights of natural persons as regards the processing of personal data, and that the cooperation and consistency procedures laid down by that regulation are respected, which it is for the referring court to determine.  
5.        
Article 58(5) of Regulation 2016/679 must be interpreted as meaning that that provision has direct effect, with the result that a national supervisory authority may rely on that provision in order to bring or continue a legal action against private parties, even where that provision has not been specifically implemented in the legislation of the Member State concerned.

ID: 3bf33d5a-c285-4409-9db4-c2aac3d9e22b

of 30 Jan 2024, C-118/22 (  
Direktor na Glavna direktsia Natsionalna politsia pri MVRSofia  
)  
Law Enforcement Directive   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
   
JUDGMENT OF THE COURT (Grand Chamber)  
30 January 2024 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data for the purpose of combating crime – Directive (EU) 2016/680 – Article 4(1)(c) and (e) – Data minimisation – Limitation of storage – Article 5 – Appropriate time limits for erasure or for a periodic review of the need for the storage – Article 10 – Processing of biometric and genetic data – Strict necessity – Article 16(2) and (3) – Right to erasure – Restriction of processing – Article 52(1) of the Charter of Fundamental Rights of the European Union – Natural person convicted by final judgment and subsequently legally rehabilitated – Storage of data until death – No right to erasure or restriction of processing – Proportionality)  
In Case C-118/22,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Varhoven administrativen sad (Supreme Administrative Court, Bulgaria), made by decision of 10 January 2022, received at the Court on 17 February 2022, in the proceedings  
NG  
v  
Direktor na Glavna direktsia ‘Natsionalna politsia’ pri Ministerstvo na vatreshnite raboti – Sofia,  
intervening parties:  
Varhovna administrativna prokuratura,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, A. Prechal, K. Jürimäe, N. Piçarra and O. Spineanu-Matei, Presidents of Chambers, M. Ilešič, J.-C. Bonichot, L.S. Rossi, I. Jarukaitis, A. Kumin, N. Jääskinen, N. Wahl and D. Gratsias (Rapporteur), Judges,  
Advocate General: P. Pikamäe,  
Registrar: R. Stefanova-Kamisheva, Administrator,  
having regard to the written procedure and further to the hearing on 7 February 2023,  
after considering the observations submitted on behalf of:  
–        NG, by P. Kuyumdzhiev, advokat  
–        the Bulgarian Government, by M. Georgieva, T. Mitova and E. Petranova, acting as Agents,  
–        the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
–        Ireland, by M. Browne, A. Joyce and M. Tierney, acting as Agents, and by D. Fennelly, Barrister-at-Law,  
–        the Spanish Government, by A. Ballesteros Panizo and J. Rodríguez de la Rúa Puig, acting as Agents,  
–        the Netherlands Government, by A. Hanje, acting as Agent,  
–        the Polish Government, by B. Majczyna, D. Łukowiak and J. Sawicka, acting as Agents,  
–        the European Commission, by A. Bouchagiar, C. Georgieva, H. Kranenborg and F. Wilman, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 15 June 2023,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 5 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89), read in conjunction with Article 13(2)(b) and (3) of that directive.  
2        The request has been made in proceedings between NG and the Direktor na Glavna direktsia ‘Natsionalna politsia’ pri Ministerstvo na vatreshnite raboti – Sofia (Director of the ‘National Police’ Directorate-General at the Bulgarian Ministry of the Interior) (‘the DGPN’) concerning the latter’s refusal of NG’s request – based on his legal rehabilitation after having been convicted by final judgment – to be removed from the national records in which the Bulgarian police authorities register persons prosecuted for an intentional criminal offence subject to public prosecution (‘the police records’).  
   
Legal context  
   
European Union law  
3        Recitals 11, 14, 26, 27, 37, 47 and 104 of Directive 2016/680 state:  
‘(11)      It is … appropriate for [the fields of judicial cooperation in criminal matters and police cooperation] to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. …  
…  
(14)      Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security … should not be considered to be activities falling within the scope of this Directive.  
…  
(26)      … It should … be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. …  
(27)      For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.  
…  
(37)      Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. …  
…  
(47)      … A natural person should also have the right to restriction of processing … where the personal data have to be maintained for purpose of evidence. In particular, instead of erasing personal data, processing should be restricted if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In such a case, restricted data should be processed only for the purpose which prevented their erasure. …  
…  
(104)      This Directive respects the fundamental rights and observes the principles recognised in the [Charter of Fundamental Rights of the European Union (‘the Charter’)] as enshrined in the TFEU, in particular the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on those rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.’  
4        Article 1 of that directive, entitled ‘Subject-matter and objectives’, provides, in paragraph 1:  
‘This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
5        Article 2 of Directive 2016/680, headed ‘Scope’, provides in paragraphs 1 and 3:  
1.      This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).  
…  
3.      This Directive does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
…’  
6        Article 3 of Directive 2016/680, headed ‘Definitions’, states:  
‘For the purposes of this Directive:  
…  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data … such as … storage …;  
…’  
7        Article 4 of Directive 2016/680, headed ‘Principles relating to processing of personal data’, provides in paragraph 1:  
‘Member States shall provide for personal data to be:  
…  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are processed;  
…  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;  
…’  
8        Article 5 of that directive, entitled ‘Time-limits for storage and review’, is worded as follows:  
‘Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.’  
9        Article 10 of that directive, entitled ‘Processing of special categories of personal data’, is worded as follows:  
‘Processing of … genetic data [and] biometric data for the purpose of uniquely identifying a natural person … shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject …’  
10      Article 13 of that directive, entitled ‘Information to be made available or given to the data subject’, provides, in paragraph 2, that, in addition to the information referred to in paragraph 1 thereof, Member States are to provide by law for the data controller to give to the data subject, in specific cases, the further information listed in that paragraph 2 to enable that person to exercise his or her rights. That additional information includes, inter alia, in point (b) of that paragraph 2, the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period. In addition, Article 13(3) of Directive 2016/680 sets out the grounds on which Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 of that article.  
11      Article 14 of Directive 2016/680, headed ‘Right of access by the data subject’, provides:  
‘Subject to Article 15, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:  
…  
(d)      where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;  
…’  
12      Article 16 of that directive, headed ‘Right to rectification or erasure of personal data and restriction of processing’, provides, in paragraphs 2 and 3:  
‘2.      Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.  
3.      Instead of erasure, the controller shall restrict processing where:  
(a)      the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or  
(b)      the personal data must be maintained for the purposes of evidence.  
…’  
13      Under Article 20 of that directive, entitled ‘Data protection by design and by default’, Member States are to provide for the data controller to implement appropriate technical and organisational measures in order to meet the requirements of that directive and protect the rights of data subjects and, inter alia, to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed.  
14      Article 29 of Directive 2016/680, entitled ‘Security of processing’, provides in paragraph 1:  
‘Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.’  
   
Bulgarian law  
   
Criminal Code  
15      Article 82(1) of the Nakazatelen kodeks (Criminal Code, DV No 26 of 2 April 1968), in the version applicable to the dispute in the main proceedings, provides:  
‘The sentence imposed shall not be enforced where:  
1.      20 years have elapsed, if the sentence is life imprisonment without the possibility of commutation or life imprisonment;  
2.      15 years have elapsed, if the sentence is a term of imprisonment of more than 10 years;  
3.      10 years have elapsed, if the sentence is a term of imprisonment of between 3 and 10 years;  
4.      5 years have elapsed, if the sentence is a term of imprisonment of less than 3 years, and  
5.      2 years have elapsed, for all other cases.’  
16      Article 85(1) of that code provides:  
‘Legal rehabilitation shall erase the conviction and shall repeal for the future the effects which the laws attach to the conviction itself, unless a law or decree provides otherwise.’  
17      Article 88a of that code is worded as follows:  
‘Where a period equal to that referred to in Article 82(1) has elapsed since the sentence was served and the convicted person has not committed a new intentional criminal offence subject to public prosecution and punishable by a term of imprisonment, the conviction and its consequences shall be erased notwithstanding any provision laid down by any other law or decree.’  
   
The Law on the Ministry of the Interior  
18      Article 26 of the Zakon za Ministerstvo na vatreshnite raboti (Law on the Ministry of the Interior, DV No 53 of 27 June 2014), in the version applicable to the dispute in the main proceedings (‘the Law on the Ministry of the Interior’), provides:  
‘(1)      When processing personal data related to activities concerning the protection of national security, combating crime, maintaining public order and the conduct of criminal proceedings, the authorities of the Ministry of the Interior:  
…  
3.      may process all necessary categories of personal data;  
…  
(2)      The time limits for data storage referred to in paragraph 1 or the time limits for a periodic review of the need to store such data shall be determined by the Ministry of the Interior. Those data shall be erased pursuant to a judicial decision or a decision by the Personal Data Protection Commission.’  
19      Under Article 27 of the Law on the Ministry of the Interior:  
‘Data taken from a person’s entry in the police records made pursuant to Article 68 shall be used only in connection with safeguarding national security, combating crime and maintaining law and order.’  
20      Article 68 of that law is worded as follows:  
‘(1)      The police authorities shall create a police record of persons who are accused of an intentional criminal offence subject to public prosecution. The authorities responsible for the investigation shall adopt the measures required for the creation of the record by the police authorities.  
(2)      The creation of the police record is a form of processing of personal data of the persons referred to in paragraph 1, which shall be carried out in accordance with the requirements of this Law.  
(3)      For the purposes of creating a police record, the police authorities shall:  
1.      collect the personal data set out in Article 18 of the Law on Bulgarian identity documents;  
2.      take a person’s fingerprints and photograph him or her;  
3.      take samples to create a person’s DNA profile.  
…  
(6)      The entry in the police records shall be erased pursuant to a written order by the personal data processing controller or by officials authorised by the controller for that purpose, of his or her own motion or following a written and reasoned application by the recorded person, where:  
1.      the record was created in breach of the law;  
2.      the criminal proceedings are discontinued, except in the cases referred to in Article 24(3) of the [Nakazatelno-protsesualen kodeks (Code of Criminal Procedure)];  
3.      the criminal proceedings resulted in an acquittal;  
4.      the person was exempted from criminal liability and an administrative penalty was imposed on that person;  
5.      the person is deceased, in which case the application may be made by that person’s heirs.  
…’  
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
21      An entry in the police records was made in respect of NG, in accordance with Article 68 of the Law on the Ministry of the Interior, in the course of a criminal investigation for failing to tell the truth as a witness, which is a criminal offence under Article 290(1) of the Criminal Code. Following that investigation, NG was charged with a criminal offence and, by judgment of 28 June 2016, confirmed on appeal by judgment of 2 December 2016, he was found guilty of that offence and given a one year suspended sentence. After serving that sentence, NG was legally rehabilitated, under Article 82(1) and Article 88a of the Criminal Code, on 14 March 2020.  
22      On 15 July 2020, on the basis of that legal rehabilitation, NG applied to the relevant district authority of the Ministry of the Interior for the erasure of the entry concerning him in the police records.  
23      By decision of 2 September 2020, the DGPN refused that application on the ground that a final criminal conviction, even in the event of legal rehabilitation, is not one of the grounds for erasure of an entry in the police records, which are exhaustively listed in Article 68(6) of the Law on the Ministry of the Interior.  
24      By decision of 2 February 2021, the Administrativen sad Sofia grad (Administrative Court of the City of Sofia, Bulgaria) dismissed the action brought by NG against that decision of the DGPN on grounds, in essence, similar to those given by the DGPN.  
25      NG brought an appeal before the referring court, the Varhoven administrativen sad (Supreme Administrative Court, Bulgaria). The main ground of that appeal alleges a breach of the principle, inferred from Articles 5, 13 and 14 of Directive 2016/680, that the processing of personal data resulting from their storage cannot be carried on indefinitely. According to NG, in essence, that is de facto the case where, in the absence of a ground for removal from the police register applicable in the event of legal rehabilitation, the data subject can never obtain the erasure of personal data collected in connection with a criminal offence for which he or she was convicted by final judgment, even after serving his or her sentence and having been legally rehabilitated.  
26      In that regard, in the first place, the referring court notes that entry in the police records constitutes the processing of personal data for the purposes set out in Article 1(1) of Directive 2016/680 and therefore falls within the scope of that directive.  
27      In the second place, it states that legal rehabilitation is not one of the grounds for removal from the police records, listed exhaustively in Article 68(6) of the Law on the Ministry of the Interior, and that none of those grounds is applicable in that situation, with the result that it is impossible for the data subject to have his entry erased from those police records in such a case.  
28      In the third place, the referring court notes that recital 26 of Directive 2016/680 refers to safeguards so that the data collected are not excessive or stored for longer than is necessary for the purposes for which they are processed and states that the data controller must set time limits for erasure or periodic review. In addition, it infers from recital 34 of that directive that processing for the purposes set out in Article 1(1) thereof should involve the restriction, erasure or destruction of those data. In its view, those principles are reflected in Article 5 and Article 13(2) and (3) of that directive.  
29      In that regard, the referring court has doubts as to whether the objectives set out in the preceding paragraph preclude national legislation which leads, for the competent authorities, to a ‘virtually unlimited right’ to data processing for the purposes set out in Article 1(1) of Directive 2016/680 and, for the data subject, to the loss of his or her right to the restriction of processing or erasure of his or her data.  
30      In those circumstances, the Varhoven administrativen sad (Supreme Administrative Court) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
‘Does the interpretation of Article 5 in conjunction with Article 13(2)(b) and (3) of [Directive 2016/680], permit national legislative measures which lead to a virtually unrestricted right of competent authorities to process personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and/or to the elimination of the data subject’s right to have the processing of his or her data restricted or to have them erased or destroyed?’  
   
Consideration of the question referred  
31      According to settled case-law, in the procedure laid down by Article 267 TFEU providing for cooperation between national courts and the Court of Justice, it is for the latter to provide the national court with an answer which will be of use to it and enable it to decide the case before it. To that end, the Court of Justice should, where necessary, reformulate the questions referred to it. The Court may also find it necessary to consider provisions of EU law which the national court has not referred to in its questions (judgment of 15 July 2021,   
Ministrstvo za obrambo  
, C-742/19, EU:C:2021:597, paragraph 31 and the case-law cited).  
32      In the present case, the referring court’s question arises from the fact that, as is apparent from the request for a preliminary ruling and from the information provided by the Bulgarian Government at the hearing before the Court, none of the grounds justifying the erasure of personal data entered in the police records, exhaustively listed by the Law on the Ministry of the Interior, is applicable in the situation at issue in the main proceedings, in which a person has been convicted by final judgment, even after his or her legal rehabilitation, with the result that those data are stored in that register and may be processed by the authorities which have access to it without any time limit other than the death of that person.  
33      In that regard, first of all, it is apparent from the order for reference, in particular from the considerations summarised in paragraph 27 above, and from the wording of the question referred itself that the referring court asks, in particular, whether the national legislation at issue in the main proceedings is compatible with the principle of proportionality. As recital 104 of Directive 2016/680 highlights, the limitations imposed by that directive on the right to the protection of personal data, provided for in Article 8 of the Charter, and on the right to respect for private and family life and the right to an effective remedy and to a fair trial, protected by Articles 7 and 47 respectively of the Charter, must be interpreted in accordance with the requirements of Article 52(1) thereof, which include respect for that principle.  
34      Next, in the wording of its question, the referring court rightly refers to Article 5 of that directive, relating to appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data. Since Article 5 is closely connected both with Article 4(1)(c) and (e) of that directive and with Article 16(2) and (3) thereof, the question referred for a preliminary ruling must be understood as also referring to those two provisions.  
35      Similarly, since the national legislation at issue in the main proceedings provides for the storage, inter alia, of biometric and genetic data, which fall within the special categories of personal data the processing of which is specifically governed by Article 10 of Directive 2016/680, it must be held that the question referred also concerns the interpretation of that provision.  
36      Lastly, the relevance of an interpretation of Article 13 of Directive 2016/680 emerges clearly from the request for a preliminary ruling only as regards paragraph 2(b) of that article. It is true, as the referring court points out, that Article 13(3) also reflects the principles set out, inter alia, in recital 26 of that directive. However, it does not appear from the file submitted to the Court that a legislative measure delaying or restricting the provision of information to the data subject, within the meaning of Article 13(3), is also at issue in the main proceedings.  
37      In the light of the foregoing, it must be held that, by its question, the referring court asks, in essence, whether Article 4(1)(c) and (e) of Directive 2016/680, read in conjunction with Articles 5 and 10, Article 13(2)(b) and Article 16(2) and (3) thereof, and in the light of Articles 7 and 8 of the Charter, must be interpreted as precluding national legislation which provides for the storage, by police authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, of personal data, including biometric and genetic data, concerning persons who have been convicted by final judgment of an intentional criminal offence subject to public prosecution, until the death of the data subject, even in the event of his or her legal rehabilitation, without also granting that person the right to have those data erased or, where appropriate, to have their processing restricted.  
38      As a preliminary point, it should be noted that the question referred concerns the processing of personal data for purposes falling, in accordance with Article 1(1) of Directive 2016/680, within the scope of that directive. It is apparent, however, from Article 27 of the Law on the Ministry of the Interior, cited in the order for reference, that the data stored in the police register may also be processed in the context of the protection of national security, to which, under Article 2(3)(a) of Directive 2016/680, read in the light of recital 14 thereof, that directive does not apply. It will therefore be for the referring court to satisfy itself that the storage of the data of the applicant in the main proceedings is not capable of serving purposes relating to the protection of national security, given that Article 2(3)(a) of Directive 2016/680 lays down an exception to the application of EU law which must be interpreted strictly (see, by analogy, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 62 and the case-law cited).  
39      In the first place, it should be borne in mind that the fundamental rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society and be weighed against other fundamental rights. Any limitation on the exercise of those fundamental rights must, in accordance with Article 52(1) of the Charter, be provided for by law, respect the essence of those fundamental rights and observe the principle of proportionality. Under the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. They must apply only in so far as is strictly necessary and the legislation which entails the limitations in question must lay down clear and precise rules governing the scope and application of those limitations (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 105 and the case-law cited).  
40      As stated, in essence, in recital 26 of Directive 2016/680, those requirements are not met where the objective of general interest pursued can reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of the persons concerned (see, by analogy, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 110 and the case-law cited).  
41      In the second place, first of all, under Article 4(1)(c) of that directive, Member States are to provide for personal data to be adequate, relevant and not excessive in relation to the purposes for which they are processed. That provision thus requires the Member States to observe the principle of ‘data minimisation’, which gives expression to the principle of proportionality (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 98 and the case-law cited).  
42      It follows that, in particular, the collection of personal data in the context of criminal proceedings and their storage by police authorities, for the purposes set out in Article 1(1) of that directive, must, like any processing falling within the scope of that directive, comply with those requirements. Such storage also constitutes an interference with the fundamental rights to respect for private life and to the protection of personal data, irrespective of whether or not the information stored is sensitive, whether or not the persons concerned have been inconvenienced in any way on account of that interference, or whether or not the stored data will subsequently be used (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 44 and the case-law cited).  
43      Furthermore, as regards, more specifically, the proportionality of the period for which the data will be stored, the Member States must, pursuant to Article 4(1)(e) of Directive 2016/680, provide that those data are to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.  
44      In that context, Article 5 of that directive requires the Member States to provide for the establishment of appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of those data and procedural measures to ensure that those time limits are observed.  
45      As stated in recital 26 of Directive 2016/680, that provision seeks to ensure that personal data are not, in accordance with the requirements of Article 4(1)(e) of that directive, kept longer than is necessary. It is true that Directive 2016/680 leaves it to the Member States to set appropriate time limits on the storage period and to decide whether those time limits concern the erasure of those data or the periodic review of the need to store them, provided that the observance of those time limits is ensured by adequate procedural measures. However, the ‘appropriate’ nature of those periods requires, in any event, that – in accordance with Article 4(1)(c) and (e) of that directive, read in the light of Article 52(1) of the Charter – those time limits allow, where appropriate, the erasure of the data concerned where their storage is no longer necessary for the purposes which justified the processing.  
46      It is, in particular, in order to enable data subjects to verify that ‘appropriate’ nature and, if necessary, to request such erasure that Article 13(2)(b) and Article 14(d) of Directive 2016/680 provide that, in principle, those persons are to be informed, where possible, of the period for which their personal data will be stored or, if that is not possible, of the criteria used to determine that period.  
47      Next, Article 10 of Directive 2016/680 constitutes a specific provision governing the processing of special categories of personal data, including biometric and genetic data. The purpose of that article is to ensure enhanced protection of the data subject, since the data in question, because of their particular sensitivity and the context in which they are processed, are liable, as is apparent from recital 37 of that directive, to create significant risks to fundamental rights and freedoms, such as the right to respect for private life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter (judgment of 26 January 2023,   
Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)  
, C-205/21, EU:C:2023:49, paragraph 116 and the case-law cited).  
48      More specifically, Article 10 of Directive 2016/680 lays down the requirement that the processing of sensitive data be allowed ‘only where strictly necessary’, which constitutes a strengthened condition for the lawful processing of such data and entails, inter alia, a particularly strict review of compliance with the principle of ‘data minimisation’, as derived from Article 4(1)(c) of Directive 2016/680; that requirement constitutes a specific application of that principle to those sensitive data (see, to that effect, judgment of 26 January 2023,   
Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police  
), C-205/21, EU:C:2023:49, paragraphs 117, 122 and 125).  
49      Lastly, Article 16(2) of Directive 2016/680 establishes a right to erasure of personal data where the processing infringes the provisions adopted pursuant to Article 4, 8 or 10 of that directive or where those data must be erased in order to comply with a legal obligation to which the data controller is subject.  
50      It follows from Article 16(2) of Directive 2016/680 that that right to erasure may be exercised, inter alia, where the storage of the personal data in question is not or is no longer necessary for the purposes for which they are processed, in breach of the provisions of national law implementing Article 4(1)(c) and (e) of that directive and, as the case may be, Article 10 thereof, or where that erasure is required in order to comply with the time limit set, for that purpose, by national law pursuant to Article 5 of that directive.  
51      However, pursuant to Article 16(3) of Directive 2016/680, national law must provide that the data controller is to restrict the processing of those data instead of erasing them where, in accordance with point (a) of that provision, the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained, or where, in accordance with point (b) of that provision, the personal data must be maintained for the purposes of evidence.  
52      It follows from the foregoing that the provisions of Directive 2016/680 examined in paragraphs 41 to 51 above establish a general framework to ensure, inter alia, that the storage of personal data and, more specifically, the period of storage, are limited to what is necessary for the purposes for which those data are stored, while leaving it to the Member States to determine, in compliance with that framework, the specific situations in which the protection of the fundamental rights of the data subject requires the erasure of those data and the time at which those data must be erased. However, as the Advocate General observed, in essence, in point 28 of his Opinion, those provisions do not require the Member States to define absolute time limits for the storage of personal data, beyond which those data must be automatically erased.  
53      In the present case, it is apparent from the documents before the Court that the personal data entered in the police records pursuant to Article 68 of the Law on the Ministry of the Interior are stored only for operational investigation purposes and, more specifically, for the purpose of comparison with other data collected during investigations into other offences.  
54      In that regard, in the first place, it should be noted that the storage, in police records, of data relating to persons who have been convicted by final judgment may prove necessary for the purposes indicated in the preceding paragraph, even after the conviction in question has been erased from the criminal record and, consequently, the effects which national legislation attaches to that conviction are repealed. Those persons may be involved in criminal offences other than those for which they were convicted or, on the contrary, they may be exonerated through the comparison of the data stored by those authorities with the data collected during the proceedings relating to those other offences.  
55      Accordingly, such storage may contribute to the objective of general interest set out in recital 27 of Directive 2016/680, which states that, for the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected (see, to that effect, judgment of 26 January 2023,   
Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)  
, C-205/21, EU:C:2023:49, paragraph 98).  
56      In the second place, it is apparent from the documents before the Court that the data stored in the police records are the data relating to the data subject referred to in the Bulgarian legislation on identity documents, his or her fingerprints, his or her photograph, a DNA sample taken for profiling purposes and, as the Bulgarian Government confirmed at the hearing, the data relating to the criminal offences committed by the data subject and to his or her convictions in that regard. Those various categories of data may prove essential for the purposes of verifying whether the data subject is involved in criminal offences other than those in respect of which he or she has been convicted by final judgment. Consequently, they may be regarded, in principle, as adequate and relevant in relation to the purposes for which they are processed, within the meaning of Article 4(1)(c) of Directive 2016/680.  
57      In the third place, the proportionality of such storage in the light of its purposes must be assessed taking into account also the appropriate technical and organisational measures laid down by national law, which are intended to ensure the confidentiality and security of the stored data with regard to processing contrary to the requirements of Directive 2016/680, in accordance with Articles 20 and 29 of that directive, and in particular the measures referred to in Article 20(2) thereof, ensuring that only personal data which are necessary for each specific purpose of the processing are processed.  
58      In the fourth place, as regards the period for which the personal data at issue in the main proceedings are stored, it is apparent, in the present case, from the request for a preliminary ruling that it is only in the event that the data subject is convicted by final judgment of an intentional criminal offence subject to public prosecution that the data in question are stored until that person’s death, since the national legislation provides for the removal of the entries of persons accused of such a criminal offence in other cases.  
59      In that regard, it must be stated, however, that the concept of an ‘intentional criminal offence subject to public prosecution’ is particularly general and is liable to apply to a large number of criminal offences, irrespective of their nature and gravity (see, to that effect, judgment of 26 January 2023,   
Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)  
, C-205/21, EU:C:2023:49, paragraph 129).  
60      As the Advocate General also observed, in essence, in points 73 and 74 of his Opinion, persons convicted by final judgment of a criminal offence falling within the scope of that concept do not all present the same degree of risk of being involved in other criminal offences, justifying a uniform period of storage of the data relating to them. Thus, in certain cases, in the light of factors such as the nature and seriousness of the offence committed or the absence of recidivism, the risk represented by the convicted person will not necessarily justify maintaining the data relating to him in the national police records provided for that purpose until his death. In such cases, there will no longer be a necessary connection between the data stored and the objective pursued (see, by analogy, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017 (EU:C:2017:592, paragraph 205). Accordingly, the storage of such data will not comply with the principle of data minimisation set out in Article 4(1)(c) of Directive 2016/680 and will exceed the period necessary for the purposes for which they are processed, contrary to Article 4(1)(e) of that directive.  
61      It must be noted, in that regard, that, admittedly, as the Advocate General stated, in essence, in point 70 of his Opinion, the legal rehabilitation of such a person, resulting in the erasure of his or her conviction from his or her criminal record, such as occurred in the main proceedings, cannot, by itself, render unnecessary the storage of his or her data in the police records, since the purposes of that storage are different from those of the recording of his or her convictions in that criminal record. However, where, as in the present case, under the applicable provisions of national criminal law, such legal rehabilitation is conditional upon the fact that the person concerned has not committed any further intentional criminal offence subject to public prosecution for a certain period of time after the sentence has been served, it may constitute an indication that the person concerned presents a lower risk with regard to the objectives of combating crime or maintaining public order and may therefore be a factor liable to reduce the period for which that storage is necessary.  
62      In the fifth place, the principle of proportionality, set out in Article 52(1) of the Charter, entails, in particular, a balancing of the importance of the objective pursued and the seriousness of the limitation placed on the exercise of the fundamental rights in question (see, to that effect, judgment of 22 November 2022,   
Luxembourg Business Registers  
, C-37/20 and C-601/20, EU:C:2022:912, paragraph 66).  
63      In the present case, as noted in paragraph 35 above, the storage of personal data in the police register at issue includes biometric and genetic data. It must therefore be pointed out that, having regard to the significant risks posed by the processing of such sensitive data to the rights and freedoms of data subjects, in particular in the context of the tasks of the competent authorities for the purposes set out in Article 1(1) of Directive 2016/680, the specific importance of the objective pursued must be assessed in the light of a number of relevant factors. Such factors include, inter alia, the fact that the processing serves a specific objective connected with the prevention of criminal offences or threats to public security displaying a certain degree of seriousness, the punishment of such offences or protection against such threats, and the specific circumstances in which that processing is carried out (judgment of 26 January 2023,   
Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)  
, C-205/21, EU:C:2023:49, paragraph 127).  
64      In that context, the Court has held that national legislation which provides for the systematic collection of the biometric and genetic data of any person accused of an intentional offence subject to public prosecution is, in principle, contrary to the requirement of strict necessity laid down in Article 10 of Directive 2016/680 and referred to in paragraph 48 above. Such legislation is liable to lead, in an indiscriminate and generalised manner, to the collection of the biometric and genetic data of most accused persons (see, to that effect, judgment of 26 January 2023,   
Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)  
, C-205/21, EU:C:2023:49, paragraphs 128 and 129).  
65      As for the European Court of Human Rights, it has held that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as provided for by the national legislation at issue in the case before that court, failed to strike a fair balance between the competing public and private interests and that, accordingly, the retention of those data constituted a disproportionate interference with the applicants’ right to respect for private life and could not be regarded as necessary in a democratic society; that interference thus constituted a violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (ECtHR, 4 December 2008,   
S. and Marper v. the United Kingdom  
, CE:ECHR:2008:1204JUD003056204, §§ 125 and 126).  
66      It is true that the storage of the biometric and genetic data of persons who have already been convicted by final judgment, even until the death of those persons, may be strictly necessary, within the meaning of Article 10 of Directive 2016/680, in particular in order to enable the possible involvement of those persons in other criminal offences to be verified and, accordingly, to prosecute and convict the perpetrators of those offences. It is necessary to have regard to the importance of that type of data for criminal investigations, even many years after the events, in particular where the offences in question constitute serious crimes (see, to that effect, ECtHR, 13 February 2020,   
Gaughran v. the United Kingdom  
, CE:ECHR:2020:0213JUD004524515, § 93).  
67      However, the storage of biometric and genetic data can be regarded as meeting the requirement that it is to be allowed only ‘where strictly necessary’, within the meaning of Article 10 of Directive 2016/680, only if it takes into consideration the nature and seriousness of the offence which led to the final criminal conviction, or other circumstances such as the particular context in which that offence was committed, its possible connection with other ongoing proceedings or the background or profile of the convicted person. Accordingly, where national legislation, such as that at issue in the main proceedings, provides that the biometric and genetic data of data subjects entered in the police records is – in the event that those persons are convicted by final judgment – to be stored until the death of those persons, the scope of that storage is, as stated in paragraphs 59 and 60 above, excessively broad with regard to the purposes for which those data are processed.  
68      In the sixth place, as regards, first, the obligation imposed on Member States to provide for the establishment of appropriate time limits, set out in Article 5 of Directive 2016/680, it should be noted that, for the reasons set out in paragraphs 59, 60 and 67 above and having regard to the requirements of Article 4(1)(c) and (e) and Article 10 of that directive, a time limit can be regarded as ‘appropriate’, within the meaning of Article 5 of that directive, in particular as regards the storage of the biometric and genetic data of any person convicted by final judgment of an intentional criminal offence subject to public prosecution, only if it takes into consideration the relevant circumstances which might require such a storage period, such as those referred to in paragraph 67 above.  
69      Consequently, even if the reference, in the national legislation, to the death of the data subject may constitute a ‘time limit’ for the erasure of stored data, within the meaning of Article 5 of Directive 2016/680, such a time limit can be regarded as ‘appropriate’ only in specific circumstances which duly justify it. That is clearly not the case where it is applicable generally and indiscriminately to any person convicted by final judgment.  
70      It is true, as pointed out in paragraph 45 above, that Article 5 of Directive 2016/680 leaves it to the Member States to decide whether time limits must be established concerning the erasure of those data or the periodic review of the need for their storage. However, it is also apparent from that paragraph that the ‘appropriate’ nature of the time limits for such a periodic review requires that they allow, in accordance with Article 4(1)(c) and (e) of that directive, read in the light of Article 52(1) of the Charter, the erasure of the data at issue, where their storage is no longer necessary. For the reasons set out in the preceding paragraph, that requirement is not satisfied where, as in the present case, the national legislation provides for such erasure, as regards a person convicted by final judgment of an intentional criminal offence subject to public prosecution, only in the event of that person’s death.  
71      As regards, secondly, the guarantees provided for in Article 16(2) and (3) of that directive, concerning the conditions relating to the rights to erasure and to the restriction of processing, it follows from paragraphs 50 and 51 above that those provisions also preclude national legislation which does not allow a person convicted by final judgment of an intentional criminal offence subject to public prosecution to exercise those rights.  
72      In the light of all the foregoing considerations, the answer to the question referred is that Article 4(1)(c) and (e) of Directive 2016/680, read in conjunction with Articles 5 and 10, Article 13(2)(b) and Article 16(2) and (3) thereof, and in the light of Articles 7 and 8 of the Charter, must be interpreted as precluding national legislation which provides for the storage, by police authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, of personal data, including biometric and genetic data, concerning persons who have been convicted by final judgment of an intentional criminal offence subject to public prosecution, until the death of the data subject, even in the event of his or her legal rehabilitation, without imposing on the data controller the obligation to review periodically whether that storage is still necessary, nor granting that data subject the right to have those data erased, where their storage is no longer necessary for the purposes for which they are processed or, where appropriate, to have the processing of those data restricted.  
   
Costs  
73      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
Article 4(1)(c) and (e) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, read in conjunction with Articles 5 and 10, Article 13(2)(b) and Article 16(2) and (3) thereof, and in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union,  
must be interpreted as precluding national legislation which provides for the storage, by police authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, of personal data, including biometric and genetic data, concerning persons who have been convicted by final judgment of an intentional criminal offence subject to public prosecution, until the death of the data subject, even in the event of his or her legal rehabilitation, without imposing on the data controller the obligation to review periodically whether that storage is still necessary, nor granting that data subject the right to have those data erased, where their storage is no longer necessary for the purposes for which they are processed or, where appropriate, to have the processing of those data restricted.

ID: 3c785cd2-a72f-46f3-8bdb-ebaf2c3e0660

Judgment of 28 Jul 2016, C-191/15 (  
Verein für Konsumenteninformation  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Territorial Scope   
   
JUDGMENT OF THE COURT (Third Chamber)  
28 July 2016 (\*)  
(Reference for a preliminary ruling — Judicial cooperation in civil matters — Regulations (EC) No 864/2007 and (EC) No 593/2008 — Consumer protection — Directive 93/13/EEC — Data protection — Directive 95/46/EC — Online sales contracts concluded with consumers resident in other Member States — Unfair terms — General terms and conditions containing a choice-of-law term applying the law of the Member State in which the company is established — Determination of the applicable law for assessing the unfairness of terms in those general terms and conditions in an action for an injunction — Determination of the law governing the processing of personal data of consumers)  
In Case C-191/15,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 9 April 2015, received at the Court on 27 April 2015, in the proceedings  
Verein für Konsumenteninformation  
v  
Amazon EU Sàrl,  
THE COURT (Third Chamber),  
composed of L. Bay Larsen (President of the Chamber), D. Švaby, J. Malenovský, M. Safjan (Rapporteur) and M. Vilaras, Judges,  
Advocate General: H. Saugmandsgaard Øe,  
Registrar: I. Illéssy, Administrator,  
having regard to the written procedure and further to the hearing on 2 March 2016,  
after considering the observations submitted on behalf of:  
–        Verein für Konsumenteninformation, by S. Langer, Rechtsanwalt,  
–        Amazon EU Sàrl, by G. Berrisch, Rechtsanwalt,  
–        the Austrian Government, by G. Eberhard, acting as Agent,  
–        the German Government, by T. Henze, A. Lippstreu, M. Hellmann, T. Laut and J. Mentgen, acting as Agents,  
–        the United Kingdom Government, by M. Holt, acting as Agent, and M. Gray, Barrister,  
–        the European Commission, by M. Wilderspin and J. Vondung, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 2 June 2016,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (OJ 2007 L 199, p. 40, ‘the Rome II Regulation’), Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (OJ 2008 L 177, p. 6, ‘the Rome I Regulation’), Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ 1993 L 95, p. 29), and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Verein für Konsumenteninformation (Association for consumer information, ‘the VKI’) and Amazon EU Sàrl, established in Luxembourg, concerning an action for an injunction brought by the VKI.  
   
Legal context  
   
EU law  
 The Rome I Regulation  
3        According to recital 7 of the Rome I Regulation:  
‘The substantive scope and the provisions of this Regulation should be consistent with Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [OJ 2001 L 12, p. 1] and [the Rome II Regulation].’  
4        Article 1(1) and (3) of the Rome I Regulation provides:  
‘1.      This Regulation shall apply, in situations involving a conflict of laws, to contractual obligations in civil and commercial matters.  
It shall not apply, in particular, to revenue, customs or administrative matters.  
...  
3.      This Regulation shall not apply to evidence and procedure, without prejudice to Article 18.’  
5        Article 4 of the Rome I Regulation, ‘Applicable law in the absence of choice’, provides:  
‘1.      To the extent that the law applicable to the contract has not been chosen in accordance with Article 3 and without prejudice to Articles 5 to 8, the law governing the contract shall be determined as follows:  
(a)      a contract for the sale of goods shall be governed by the law of the country where the seller has his habitual residence;  
(b)      a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence;  
(c)      a contract relating to a right   
in rem  
 in immovable property or to a tenancy of immovable property shall be governed by the law of the country where the property is situated;  
(d)      notwithstanding point (c), a tenancy of immovable property concluded for temporary private use for a period of no more than six consecutive months shall be governed by the law of the country where the landlord has his habitual residence, provided that the tenant is a natural person and has his habitual residence in the same country;  
(e)      a franchise contract shall be governed by the law of the country where the franchisee has his habitual residence;  
(f)      a distribution contract shall be governed by the law of the country where the distributor has his habitual residence;  
(g)      a contract for the sale of goods by auction shall be governed by the law of the country where the auction takes place, if such a place can be determined;  
(h)      a contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments, as defined by Article 4(1), point (17) of Directive 2004/39/EC [of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (OJ 2004 L 145, p. 1)], in accordance with non-discretionary rules and governed by a single law, shall be governed by that law.  
2.      Where the contract is not covered by paragraph 1 or where the elements of the contract would be covered by more than one of points (a) to (h) of paragraph 1, the contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence.  
3.      Where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply.  
4.      Where the law applicable cannot be determined pursuant to paragraphs 1 or 2, the contract shall be governed by the law of the country with which it is most closely connected.’  
6        Article 6 of the Rome I Regulation, ‘Consumer contracts’, reads as follows:  
‘1.      Without prejudice to Articles 5 and 7, a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the consumer) with another person acting in the exercise of his trade or profession (the professional) shall be governed by the law of the country where the consumer has his habitual residence, provided that the professional:  
(a)      pursues his commercial or professional activities in the country where the consumer has his habitual residence, or  
(b)      by any means, directs such activities to that country or to several countries including that country,  
and the contract falls within the scope of such activities.  
2.      Notwithstanding paragraph 1, the parties may choose the law applicable to a contract which fulfils the requirements of paragraph 1, in accordance with Article 3. Such a choice may not, however, have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which, in the absence of choice, would have been applicable on the basis of paragraph 1.  
...’  
7        Article 9 of the regulation, ‘Overriding mandatory provisions’, states:  
‘1.      Overriding mandatory provisions are provisions the respect for which is regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation, to such an extent that they are applicable to any situation falling within their scope, irrespective of the law otherwise applicable to the contract under this Regulation.  
2.      Nothing in this Regulation shall restrict the application of the overriding mandatory provisions of the law of the forum.  
3.      Effect may be given to the overriding mandatory provisions of the law of the country where the obligations arising out of the contract have to be or have been performed, in so far as those overriding mandatory provisions render the performance of the contract unlawful. In considering whether to give effect to those provisions, regard shall be had to their nature and purpose and to the consequences of their application or non-application.’  
8        In accordance with Article 10 of the regulation, ‘Consent and material validity’:  
1.      The existence and validity of a contract, or of any term of a contract, shall be determined by the law which would govern it under this Regulation if the contract or term were valid.  
2.      Nevertheless, a party, in order to establish that he did not consent, may rely upon the law of the country in which he has his habitual residence if it appears from the circumstances that it would not be reasonable to determine the effect of his conduct in accordance with the law specified in paragraph 1.’  
9        Article 23 of the regulation, ‘Relationship with other provisions of Community law’, provides:  
‘With the exception of Article 7, this Regulation shall not prejudice the application of provisions of Community law which, in relation to particular matters, lay down conflict-of-law rules relating to contractual obligations.’  
 The Rome II Regulation  
10      According to recitals 7 and 21 of the Rome II Regulation:  
‘(7)      The substantive scope and the provisions of this Regulation should be consistent with [Regulation No 44/2001] and the instruments dealing with the law applicable to contractual obligations.  
...  
(21)      The special rule in Article 6 is not an exception to the general rule in Article 4(1) but rather a clarification of it. In matters of unfair competition, the conflict-of-law rule should protect competitors, consumers and the general public and ensure that the market economy functions properly. The connection to the law of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected generally satisfies these objectives.’  
11      Article 1(1) and (3) of the Rome II Regulation provides:  
‘1.      This Regulation shall apply, in situations involving a conflict of laws, to non-contractual obligations in civil and commercial matters. It shall not apply, in particular, to revenue, customs or administrative matters or to the liability of the State for acts and omissions in the exercise of State authority (  
acta iure imperii  
).  
...  
3.      This Regulation shall not apply to evidence and procedure, without prejudice to Articles 21 and 22.’  
12      In accordance with Article 4 of the Rome II Regulation, ‘General rule’, which is in Chapter II of the regulation, ‘Torts/Delicts’:  
‘1.      Unless otherwise provided for in this Regulation, the law applicable to a non-contractual obligation arising out of a tort/delict shall be the law of the country in which the damage occurs irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur.  
2.      However, where the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply.  
3.      Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question.’  
13      Article 6 of the Rome II Regulation, ‘Unfair competition and acts restricting free competition’, which is also in Chapter II of the regulation, reads as follows:  
‘1.      The law applicable to a non-contractual obligation arising out of an act of unfair competition shall be the law of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected.  
2.      Where an act of unfair competition affects exclusively the interests of a specific competitor, Article 4 shall apply.  
3.      (a)   The law applicable to a non-contractual obligation arising out of a restriction of competition shall be the law of the country where the market is, or is likely to be, affected.  
(b)      When the market is, or is likely to be, affected in more than one country, the person seeking compensation for damage who sues in the court of the domicile of the defendant, may instead choose to base his or her claim on the law of the court seised, provided that the market in that Member State is amongst those directly and substantially affected by the restriction of competition out of which the non-contractual obligation on which the claim is based arises; where the claimant sues, in accordance with the applicable rules on jurisdiction, more than one defendant in that court, he or she can only choose to base his or her claim on the law of that court if the restriction of competition on which the claim against each of these defendants relies directly and substantially affects also the market in the Member State of that court.  
4.      The law applicable under this Article may not be derogated from by an agreement pursuant to Article 14.’  
14      Article 14 of the Rome II Regulation, ‘Freedom of choice’, provides:  
‘1.      The parties may agree to submit non-contractual obligations to the law of their choice:  
(a)      by an agreement entered into after the event giving rise to the damage occurred;  
or  
(b)      where all the parties are pursuing a commercial activity, also by an agreement freely negotiated before the event giving rise to the damage occurred.  
The choice shall be expressed or demonstrated with reasonable certainty by the circumstances of the case and shall not prejudice the rights of third parties.  
2.      Where all the elements relevant to the situation at the time when the event giving rise to the damage occurs are located in a country other than the country whose law has been chosen, the choice of the parties shall not prejudice the application of provisions of the law of that other country which cannot be derogated from by agreement.  
3.      Where all the elements relevant to the situation at the time when the event giving rise to the damage occurs are located in one or more of the Member States, the parties’ choice of the law applicable other than that of a Member State shall not prejudice the application of provisions of Community law, where appropriate as implemented in the Member State of the forum, which cannot be derogated from by agreement.’  
15      In accordance with Article 16 of the regulation, ‘Overriding mandatory provisions’:  
‘Nothing in this Regulation shall restrict the application of the provisions of the law of the forum in a situation where they are mandatory irrespective of the law otherwise applicable to the non-contractual obligation.’  
 Regulation (EC) No 2006/2004  
16      Article 3, ‘Definitions’, of Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation) (OJ 2004 L 364, p. 1) provides:  
‘For the purposes of this Regulation:  
...  
(b)      “intra-Community infringement” means any act or omission contrary to the laws that protect consumers’ interests, as defined in (a), that harms, or is likely to harm, the collective interests of consumers residing in a Member State or Member States other than the Member State where the act or omission originated or took place; or where the responsible seller or supplier is established; or where evidence or assets pertaining to the act or omission are to be found;  
...’  
17      Article 4 of that regulation, ‘Competent authorities’, states:  
‘1.      Each Member State shall designate the competent authorities and a single liaison office responsible for the application of this Regulation.  
2.      Each Member State may, if necessary in order to fulfil its obligations under this Regulation, designate other public authorities. They may also designate bodies having a legitimate interest in the cessation or prohibition of intra-Community infringements in accordance with Article 8(3).  
3.      Each competent authority shall, without prejudice to paragraph 4, have the investigation and enforcement powers necessary for the application of this Regulation and shall exercise them in conformity with national law.  
4.      The competent authorities may exercise the powers referred to in paragraph 3 in conformity with national law either:  
(a)      directly under their own authority or under the supervision of the judicial authorities; or  
(b)      by application to courts competent to grant the necessary decision, including, where appropriate, by appeal, if the application to grant the necessary decision is not successful.  
5.      Insofar as competent authorities exercise their powers by application to the courts in accordance with paragraph 4(b), those courts shall be competent to grant the necessary decisions.  
6.      The powers referred to in paragraph 3 shall only be exercised where there is a reasonable suspicion of an intra-Community infringement and shall include, at least, the right:  
(a)      to have access to any relevant document, in any form, related to the intra-Community infringement;  
(b)      to require the supply by any person of relevant information related to the intra-Community infringement;  
(c)      to carry out necessary on-site inspections;  
(d)      to request in writing that the seller or supplier concerned cease the intra-Community infringement;  
(e)      to obtain from the seller or supplier responsible for intra-Community infringements an undertaking to cease the intra-Community infringement; and, where appropriate, to publish the resulting undertaking;  
(f)      to require the cessation or prohibition of any intra-Community infringement and, where appropriate, to publish resulting decisions;  
(g)      to require the losing defendant to make payments into the public purse or to any beneficiary designated in or under national legislation, in the event of failure to comply with the decision.  
...’  
 Directive 2009/22/EC  
18      Article 2(2) of Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers’ interests (OJ 2009 L 110, p. 30) provides:  
‘This Directive shall be without prejudice to the rules of private international law with respect to the applicable law, that is, normally, either the law of the Member State where the infringement originated or the law of the Member State where the infringement has its effects.’  
 Directive 93/13  
19      According to the fifth and sixth recitals of Directive 93/13:  
‘Whereas, generally speaking, consumers do not know the rules of law which, in Member States other than their own, govern contracts for the sale of goods or services; whereas this lack of awareness may deter them from direct transactions for the purchase of goods or services in another Member State;  
Whereas, in order to facilitate the establishment of the internal market and to safeguard the citizen in his role as consumer when acquiring goods and services under contracts which are governed by the laws of Member States other than his own, it is essential to remove unfair terms from those contracts.’  
20      Article 3 of Directive 93/13 provides:  
‘1.      A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer.  
...  
3.      The Annex shall contain an indicative and non-exhaustive list of the terms which may be regarded as unfair.’  
21      Under Article 5 of that directive:  
‘In the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail. This rule on interpretation shall not apply in the context of the procedures laid down in Article 7(2).’  
22      Article 6 of the directive states:  
‘1.      Member States shall lay down that unfair terms used in a contract concluded with a consumer by a seller or supplier shall, as provided for under their national law, not be binding on the consumer and that the contract shall continue to bind the parties upon those terms if it is capable of continuing in existence without the unfair terms.  
2.      Member States shall take the necessary measures to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of the law of a non-Member country as the law applicable to the contract if the latter has a close connection with the territory of the Member States.’  
23      Article 7 of the directive reads as follows:  
‘1.      Member States shall ensure that, in the interests of consumers and of competitors, adequate and effective means exist to prevent the continued use of unfair terms in contracts concluded with consumers by sellers or suppliers.  
2.      The means referred to in paragraph 1 shall include provisions whereby persons or organisations, having a legitimate interest under national law in protecting consumers, may take action according to the national law concerned before the courts or before competent administrative bodies for a decision as to whether contractual terms drawn up for general use are unfair, so that they can apply appropriate and effective means to prevent the continued use of such terms.  
...’  
24      In accordance with Article 8 of the directive:  
‘Member States may adopt or retain the most stringent provisions compatible with the Treaty in the area covered by this Directive, to ensure a maximum degree of protection for the consumer.’  
25      The annex to Directive 93/13 lists the terms referred to in Article 3(3) of the directive. Point 1(q) of the annex reads as follows:  
‘Terms which have the object or effect of:  
...  
(q)      excluding or hindering the consumer’s right to take legal action or exercise any other legal remedy ...’  
 Directive 95/46  
26      Article 4 of Directive 95/46, ‘National law applicable’, provides:  
‘1.      Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:  
(a)      the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;  
(b)      the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;  
(c)      the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.  
2.      In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.’  
   
Austrian law  
27      Paragraph 6 of the Konsumentenschutzgesetz (Law on consumer protection) of 8 March 1979 (BGBl. 140/1979), headed ‘Unlawful contractual terms’, provides in subparagraph 3 that a contractual provision included in general terms and conditions or pre-printed contractual forms is to be ineffective if it is unclear or unintelligible.  
28      Under Paragraph 13a of that law, Paragraph 6 of the law is to apply for the purposes of consumer protection regardless of the law applicable to the contract, where the contract was entered into in connection with an activity of an operator or his agents pursued in Austria and directed towards the conclusion of contracts of that kind.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
29      Amazon EU is a company established in Luxembourg belonging to an international mail order group which, among other activities, via a website with a domain name with the extension .de, addresses consumers residing in Austria, with whom it concludes electronic sales contracts. The company has no registered office or establishment in Austria.  
30      Until mid-2012 the general terms and conditions in the contracts concluded with those consumers were worded as follows:  
‘1.      Terms of the purchaser that differ from these will not be recognised by Amazon.de unless it has expressly agreed in writing to their application.  
...  
6.      In the case of payment on receipt of invoice and in other cases where there are legitimate grounds for doing so, Amazon.de will check and evaluate the data provided by the purchaser and exchange data with other firms in the Amazon group, economic information agencies and, where appropriate, with Bürgel Wirtschaftsinformationen GmbH & Co. KG, Postfach 5001 66, 22701 Hamburg, Germany.  
...  
9.      In our decisions on use of payment on receipt of invoice we use — in addition to our own data — probability values to assess the risk of default which we obtain from Bürgel Wirtschaftsinformationen GmbH & Co. KG, Gasstraße 18, 22761 Hamburg, and informa Solutions GmbH, Rheinstraße 99, 76532 Baden-Baden [(Germany)]. ... The firms specified are also used to validate the address data you supply.  
...  
11.      If the user chooses to provide content on Amazon.de (e.g. customer reviews), he shall grant Amazon.de for the duration of the underlying right an exclusive licence without any limitation with regard to time or place to make further use of the content for any purpose whatsoever both online and offline.  
12.      Luxembourg law shall apply, excluding [the United Nations Convention on the International Sale of Goods].’  
31      The VKI, which is an entity qualified to bring actions for injunctions within the meaning of Directive 2009/22, brought an action before the Austrian courts for an injunction to prohibit the use of all the terms in those general terms and conditions and for publication of the judgment to be delivered, as it considered that those terms were all contrary to legal prohibitions or accepted principles of morality.  
32      The court at first instance allowed all the claims in the action with the exception of the claim relating to clause 8, concerning the payment of an additional charge for payment on receipt of invoice. It presumed that in principle the Rome I Regulation applies and, on the basis of Article 6(2) of that regulation, held that clause 12 on the choice of applicable law was invalid, on the ground that the choice of law should not have the result of depriving consumers of the protection afforded to them by the law of their State of habitual residence. The court concluded therefrom that the validity of the other terms had to be assessed in the light of Austrian law. Finally, in relation to clauses 6, 9 and 11, the court observed that only the data protection issues had to be assessed in the light of the relevant Luxembourg law, since the Rome I Regulation does not exclude the application of Directive 95/46.  
33      The appellate court, to which both parties to the main proceedings appealed, set aside the judgment of the first-instance court and referred the case back to it for rehearing. It considered that the Rome I Regulation was relevant for the determination of the applicable law, and only made a substantive examination of clause 12 on the choice of applicable law. It held that Article 6(2) of the regulation did not allow the conclusion that that term was unlawful, and that in accordance with Article 10(1) of the regulation that term should instead have been assessed in the light of Luxembourg law. Inviting the first-instance court to carry out that assessment, the appellate court observed that, if that term proved to be valid as a matter of Luxembourg law, the other terms would also have to be assessed according to that law, and a comparison with Austrian law would then have to be made in order to determine which law was more favourable for the purposes of Article 6(2) of the Rome I Regulation.  
34      The Oberster Gerichtshof (Supreme Court, Austria), to which the VKI appealed, is uncertain as to the law applicable in the main proceedings. In those circumstances it decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Must the law applicable to an action for an injunction within the meaning of [Directive 2009/22] be determined in accordance with Article 4 of [the Rome II Regulation] where the action is directed against the use of unfair contract terms by an undertaking established in a Member State which in the course of electronic commerce concludes contracts with consumers resident in other Member States, in particular in the State of the court seised?  
(2)      If Question 1 is answered in the affirmative:  
(a)      Must the country in which the damage occurs (Article 4(1) of the Rome II Regulation) be understood as every State towards which the commercial activities of the defendant undertaking are directed, so that the terms challenged must be assessed according to the law of the State of the court seised if the qualified entity challenges the use of those terms in commerce with consumers resident in that State?  
(b)      Does a manifestly closer connection (Article 4(3) of the Rome II Regulation) with the law of the State in which the defendant undertaking is established exist where that undertaking’s terms and conditions provide that the law of that State is to apply to contracts concluded by the undertaking?  
(c)      Does a choice-of-law term of that kind entail on other grounds that the contractual terms challenged must be assessed in accordance with the law of the State in which the defendant undertaking is established?  
(3)      If Question 1 is answered in the negative:  
How then must the law applicable to the action for an injunction be determined?  
(4)      Regardless of the answers to the above questions:  
(a)      Is a term included in general terms and conditions under which a contract concluded in the course of electronic commerce between a consumer and an operator established in another Member State is to be subject to the law of the State in which that operator is established unfair within the meaning of Article 3(1) of [Directive 93/13]?  
(b)      Is the processing of personal data by an undertaking which in the course of electronic commerce concludes contracts with consumers resident in other Member States, in accordance with Article 4(1)(a) of [Directive 95/46], regardless of the law that would otherwise apply, subject exclusively to the law of the Member State in which is situated the establishment of the undertaking in the context of which the processing takes place, or must the undertaking also comply with the data protection rules of those Member States to which its commercial activities are directed?’  
   
Consideration of the questions referred  
   
Questions 1 to 3  
35      By its first three questions, which should be considered together, the referring court essentially seeks to know how the Rome I and Rome II Regulations should be interpreted for the purpose of determining the law or laws applicable to an action for an injunction within the meaning of Directive 2009/22 brought against the use of allegedly unlawful contractual terms by an undertaking established in one Member State which concludes contracts by way of electronic commerce with consumers resident in other Member States, in particular in the State of the court seised.  
36      As a preliminary point, it should be observed that, as regards the respective scopes of the Rome I and Rome II Regulations, the concepts of ‘contractual obligation’ and ‘non-contractual obligation’ in those regulations must be interpreted independently by reference primarily to the regulations’ scheme and purpose. Account should also be taken, in accordance with recital 7 of each of those regulations, of the aim that those regulations should be applied consistently with each other and with Regulation No 44/2001 (‘the Brussels I Regulation’), which inter alia draws a distinction in Article 5 between matters relating to contract and matters relating to tort, delict and quasi-delict (see judgment of 21 January 2016 in   
ERGO Insurance and Gjensidige Baltic  
, C-359/14 and C-475/14, EU:C:2016:40, paragraph 43).  
37      As regards the concept of ‘non-contractual obligation’ within the meaning of Article 1 of the Rome II Regulation, it must be recalled that the concept of ‘matters relating to tort, delict and quasi-delict’ within the meaning of Article 5(3) of the Brussels I Regulation includes all actions which seek to establish the liability of a defendant and are not related to a ‘contract’ within the meaning of Article 5(1) of the Brussels I Regulation (judgment of 21 January 2016 in   
ERGO Insurance and Gjensidige Baltic  
, C-359/14 and C-475/14, EU:C:2016:40, paragraph 45).  
38      In the context of the Convention of 27 September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (OJ 1978 L 304, p. 36, ‘the Brussels Convention’), the Court has held that a preventive action brought by a consumer protection association for the purpose of preventing a trader from using terms considered to be unfair in contracts with private individuals is a matter relating to tort, delict or quasi-delict within the meaning of Article 5(3) of the convention (judgment of 1 October 2002 in   
Henkel  
, C-167/00, EU:C:2002:555, paragraph 50), that interpretation also being valid for the Brussels I Regulation (see, to that effect, judgment of 13 March 2014 in   
Brogsitter  
, C-548/12, EU:C:2014:148, paragraph 19).  
39      In the light of the aim of consistent application mentioned in paragraph 36 above, the view that, in matters of consumer protection, non-contractual liability extends also to the undermining of legal stability by the use of unfair terms which it is the task of consumer protection associations to prevent (see, to that effect, judgment of 1 October 2002 in   
Henkel  
, C-167/00, EU:C:2002:555, paragraph 42) is fully applicable to the interpretation of the Rome I and Rome II Regulations. It must therefore be considered that an action for an injunction under Directive 2009/22 relates to a non-contractual obligation arising out of a tort/delict within the meaning of Chapter II of the Rome II Regulation.  
40      Article 6(1) of the Rome II Regulation, which forms part of Chapter II of the regulation, provides, as a special rule relating to non-contractual obligations arising out of an act of unfair competition, for the application of the law of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected.  
41      It follows from recital 21 of the Rome II Regulation that Article 6(1) expresses, in the specific field of unfair competition, the   
lex loci damni  
 principle laid down in Article 4(1) of the regulation.  
42      As the Advocate General observes in point 73 of his Opinion, unfair competition within the meaning of Article 6(1) of the Rome II Regulation covers the use of unfair terms inserted into general terms and conditions, as this is likely to affect the collective interests of consumers as a group and hence to influence the conditions of competition on the market.  
43      In the case of an action for an injunction referred to in Directive 2009/22, the country in which the collective interests of consumers are affected within the meaning of Article 6(1) of the Rome II Regulation is the country of residence of the consumers to whom the undertaking directs its activities and whose interests are defended by the relevant consumer protection association by means of that action.  
44      It should be stated that Article 4(3) of the Rome II Regulation, under which the law of another country applies if it is clear from all the circumstances that the tort/delict is manifestly more closely connected with a country other than that indicated in Article 4(1) of the regulation, cannot lead to a different result.  
45      As the Advocate General notes in point 77 of his Opinion, the alternative rule in Article 4(3) of the Rome II Regulation is not suited to the matter of unfair competition, since Article 6(1) of the regulation aims to protect collective interests — more extensive than the relations between the parties to the dispute — by providing for a rule specifically suited to that purpose. That aim would not be achieved if it were permissible to block the rule on the basis of personal connections between those parties.  
46      In any event, the fact that Amazon EU provides in its general terms and conditions that the law of the country in which it is established is to apply to the contracts it concludes cannot legitimately constitute such a manifestly closer connection.  
47      If it were otherwise, a professional such as Amazon EU would de facto be able, by means of such a term, to choose the law to which a non-contractual obligation is subject, and could thereby evade the conditions set out in that respect in Article 14(1)(a) of the Rome II Regulation.  
48      Consequently, the law applicable to an action for an injunction within the meaning of Directive 2009/22 must be determined, without prejudice to Article 1(3) of the Rome II Regulation, in accordance with Article 6(1) of that regulation, where what is alleged is a breach of a law aimed at protecting consumers’ interests with respect to the use of unfair terms in general terms and conditions.  
49      On the other hand, the law applicable to the examination of the unfairness of terms in consumer contracts which are the subject of an action for an injunction must be determined independently in accordance with the nature of those terms. Thus, where the action for an injunction aims to prevent such terms from being included in consumer contracts in order to create contractual obligations, the law applicable to the assessment of the terms must be determined in accordance with the Rome I Regulation.  
50      In the present case, the allegedly unfair terms which are the subject of the action for an injunction in the main proceedings are, for the consumers to whom they are addressed, in the nature of contractual obligations within the meaning of Article 1(1) of the Rome I Regulation.  
51      That conclusion is not affected by the collective nature of the action by means of which the validity of the terms is challenged. The fact that the action does not concern individual contracts actually concluded is inherent in the very nature of such a preventive collective action, in which an abstract review is carried out.  
52      A distinction must therefore be drawn, for the purposes of determining the applicable law, between the assessment of the terms concerned, on the one hand, and, on the other hand, the action for an injunction to prohibit the use of those terms brought by an association such as the VKI.  
53      That distinction is necessary to ensure the uniform application of the Rome I and Rome II Regulations. Furthermore, the independent attachment of the terms in question ensures that the applicable law does not vary according to the kind of action chosen.  
54      If, in a collective action, the contractual terms concerned had to be examined in the light of the law designated as applicable under Article 6(1) of the Rome II Regulation, there would be a risk that the criteria of examination would be different from those used in an individual action brought by a consumer.  
55      In the examination of terms in an individual action brought by a consumer, the law designated as applicable as the law of the contract may be different from the law designated as applicable to an action for an injunction as the law of the tort or delict. It must be observed in this respect that the level of protection of consumers still varies from one Member State to another, in accordance with Article 8 of Directive 93/13, so that the assessment of a term may vary, other things being equal, according to the applicable law.  
56      Such a different attachment, as regards the law designated as applicable, of a term depending on the kind of action brought would have the effect in particular of abolishing the consistency of assessment between collective actions and individual actions which the Court has established by requiring the national courts of their own motion to draw, including for the future, all the conclusions provided for in national law that follow from the finding, in an action for an injunction, that a term included in the general terms and conditions of consumer contracts is unfair, in order that such a term should not bind consumers who have concluded a contract containing those general terms and conditions (see judgment of 26 April 2012 in   
Invitel  
, C-472/10, EU:C:2012:242, paragraph 43).  
57      The inconsistency that would result from a term having a different attachment depending on the kind of action brought would jeopardise the objective pursued by Directives 2009/22 and 93/13 of efficaciously putting an end to the use of unfair terms.  
58      It follows from the above that the law applicable to an action for an injunction within the meaning of Directive 2009/22 must be determined in accordance with Article 6(1) of the Rome II Regulation where what is alleged is a breach of a law aimed at protecting consumers’ interests with respect to the use of unfair terms in general terms and conditions, whereas the law applicable to the assessment of a particular contractual term must always be determined pursuant to the Rome I Regulation, whether this is in an individual action or in a collective action.  
59      However, it should be stated that, where in an action for an injunction an assessment is being made of whether a particular contractual term is unfair, it follows from Article 6(2) of the Rome I Regulation that the choice of the applicable law is without prejudice to the application of the mandatory provisions laid down by the law of the country of residence of the consumers whose interests are being defended by means of that action. Those provisions may include the provisions transposing Directive 93/13, provided that they ensure a higher level of protection for the consumer, in accordance with Article 8 of that directive.  
60      The answer to the first three questions is therefore that the Rome I and Rome II Regulations must be interpreted as meaning that, without prejudice to Article 1(3) of each of those regulations, the law applicable to an action for an injunction within the meaning of Directive 2009/22 directed against the use of allegedly unfair contractual terms by an undertaking established in a Member State which concludes contracts in the course of electronic commerce with consumers resident in other Member States, in particular in the State of the court seised, must be determined in accordance with Article 6(1) of the Rome II Regulation, whereas the law applicable to the assessment of a particular contractual term must always be determined pursuant to the Rome I Regulation, whether that assessment is made in an individual action or in a collective action.  
   
Question 4(a)  
61      By Question 4(a) the referring court seeks to know whether a term in the general terms and conditions of a contract concluded in the course of electronic commerce between a seller or supplier and a consumer, under which the contract is to be governed by the law of the Member State in which the seller or supplier is established, is unfair within the meaning of Article 3(1) of Directive 93/13.  
62      In accordance with that provision, a contractual term which has not been individually negotiated must be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations to the detriment of the consumer.  
63      Article 3(2) of Directive 93/13 specifies that a term must always be regarded as not individually negotiated where it has been drafted in advance by the seller or supplier and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract. As the Advocate General observes in point 84 of his Opinion, general terms and conditions such as those at issue in the main proceedings correspond to that description.  
64      Under Article 4(1) of Directive 93/13, a contractual term may be declared unfair only after a case-by-case examination of all the relevant circumstances, including the nature of the goods or services which are the subject of the contract.  
65      It is for the national court to determine whether, having regard to the particular circumstances of the case, a term meets the requirements of good faith, balance and transparency. The Court nonetheless has jurisdiction to elicit from the provisions of Directive 93/13 the criteria that the national court may or must apply when making such an examination (see, to that effect, judgment of 30 April 2014 in   
Kásler and Káslerné Rábai  
, C-26/13, EU:C:2014:282, paragraphs 40 and 45 and the case-law cited).  
66      In the case of a term such as clause 12 of the general terms and conditions at issue in the main proceedings, concerning the applicable law, it must first be observed that EU legislation in principle allows choice-of-law terms. Article 6(2) of the Rome I Regulation provides that the parties may choose the law applicable to a consumer contract, provided that the protection is ensured which the consumer is afforded by provisions of the law of his country that cannot be derogated from by agreement.  
67      In those circumstances, as the Advocate General observes in point 94 of his Opinion, a pre-formulated term on the choice of the applicable law designating the law of the Member State in which the seller or supplier is established is unfair only in so far as it displays certain specific characteristics inherent in its wording or context which cause a significant imbalance in the rights and obligations of the parties.  
68      In particular, the unfairness of such a term may result from a formulation that does not comply with the requirement of being drafted in plain and intelligible language set out in Article 5 of Directive 93/13. That requirement must, having regard to the consumer’s weak position vis-à-vis the seller or supplier with respect in particular to his level of knowledge, be interpreted broadly (see, to that effect, judgment of 23 April 2015 in   
Van Hove  
, C-96/14, EU:C:2015:262, paragraph 40 and the case-law cited).  
69      Furthermore, where the effects of a term are specified by mandatory statutory provisions, it is essential that the seller or supplier informs the consumer of those provisions (see, to that effect, judgment of 26 April 2012 in   
Invitel  
, C-472/10, EU:C:2012:242, paragraph 29). That is the case of Article 6(2) of the Rome I Regulation, which provides that the choice of applicable law must not have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which would have been applicable in the absence of choice.  
70      Having regard to the mandatory nature of the requirement in Article 6(2) of the Rome I Regulation, the court faced with a choice-of-applicable-law term will, where a consumer with his principal residence in Austria is involved, have to apply those Austrian statutory provisions which, under Austrian law, cannot be derogated from by agreement. It will be for the referring court to identify those provisions if need be.  
71      The answer to Question 4(a) is therefore that Article 3(1) of Directive 93/13 must be interpreted as meaning that a term in the general terms and conditions of a seller or supplier which has not been individually negotiated, under which the contract concluded with a consumer in the course of electronic commerce is to be governed by the law of the Member State in which the seller or supplier is established, is unfair in so far as it leads the consumer into error by giving him the impression that only the law of that Member State applies to the contract, without informing him that under Article 6(2) of the Rome I Regulation he also enjoys the protection of the mandatory provisions of the law that would be applicable in the absence of that term, this being for the national court to ascertain in the light of all the relevant circumstances.  
   
Question 4(b)  
72      By Question 4(b) the referring court seeks essentially to know whether Article 4(1)(a) of Directive 95/46 must be interpreted as meaning that the treatment of personal data by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities.  
73      In accordance with Article 4(1)(a) of Directive 95/46, each Member State is to apply the national provisions it adopts pursuant to that directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.  
74      It follows that the processing of data in the context of the activities of an establishment is governed by the law of the Member State in whose territory that establishment is situated.  
75      As regards, first, the concept of ‘establishment’ for the purposes of Article 4(1)(a) of Directive 95/46, the Court has previously held that it extends to any real and effective activity, even a minimal one, exercised through stable arrangements (judgment of 1 October 2015 in   
Weltimmo  
, C-230/14, EU:C:2015:639, paragraph 31).  
76      As the Advocate General states in point 119 of his Opinion, while the fact that the undertaking responsible for the data processing does not have a branch or subsidiary in a Member State does not preclude it from having an establishment there within the meaning of Article 4(1)(a) of Directive 95/46, such an establishment cannot exist merely because the undertaking’s website is accessible there.  
77      Rather, as the Court has previously held, both the degree of stability of the arrangements and the effective exercise of activities in the Member State in question must be assessed (see, to that effect, judgment of 1 October 2015 in   
Weltimmo  
, C-230/14, EU:C:2015:639, paragraph 29).  
78      As regards, second, the question whether the processing of personal data concerned is carried out ‘in the context of the activities’ of that establishment within the meaning of Article 4(1)(a) of Directive 95/46, the Court has pointed out that that provision requires the processing of personal data in question to be carried out not ‘by’ the establishment concerned itself but only ‘in the context of the activities’ of the establishment (judgment of 1 October 2015 in   
Weltimmo  
, C-230/14, EU:C:2015:639, paragraph 35).  
79      It is for the national court to determine, in the light of that case-law and taking account of all the relevant circumstances of the case at issue in the main proceedings, whether Amazon EU carries out the data processing in question in the context of the activities of an establishment situated in a Member State other than Luxembourg.  
80      As the Advocate General observes in point 128 of his Opinion, if the referring court were to conclude that the establishment in the context of which Amazon EU carries out the processing of that data is situated in Germany, it would be for German law to govern the processing.  
81      In the light of the foregoing, the answer to Question 4(b) is that Article 4(1)(a) of Directive 95/46 must be interpreted as meaning that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State. It is for the national court to ascertain whether that is the case.  
   
Costs  
82      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) and Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) must be interpreted as meaning that, without prejudice to Article 1(3) of each of those regulations, the law applicable to an action for an injunction within the meaning of Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers’ interests directed against the use of allegedly unfair contractual terms by an undertaking established in a Member State which concludes contracts in the course of electronic commerce with consumers resident in other Member States, in particular in the State of the court seised, must be determined in accordance with Article 6(1) of Regulation No 864/2007, whereas the law applicable to the assessment of a particular contractual term must always be determined pursuant to Regulation No 593/2008, whether that assessment is made in an individual action or in a collective action.  
2.        
Article 3(1) of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts must be interpreted as meaning that a term in the general terms and conditions of a seller or supplier which has not been individually negotiated, under which the contract concluded with a consumer in the course of electronic commerce is to be governed by the law of the Member State in which the seller or supplier is established, is unfair in so far as it leads the consumer into error by giving him the impression that only the law of that Member State applies to the contract, without informing him that under Article 6(2) of Regulation No 593/2008 he also enjoys the protection of the mandatory provisions of the law that would be applicable in the absence of that term, this being for the national court to ascertain in the light of all the relevant circumstances.  
3.        
Article 4(1)(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State. It is for the national court to ascertain whether that is the case.

ID: 4277954b-f090-48c4-970d-88f091251d79

Judgment of 11 Dec 2014, C-212/13 (  
Ryneš  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Processing   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Household exemption   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
 Information to be provided in case of indirect collection   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
   
JUDGMENT OF THE COURT (Fourth Chamber)  
11 December 2014 (\*)  
(Reference for a preliminary ruling — Directive 95/46/EC — Protection of individuals — Processing of personal data — Concept of ‘in the course of a purely personal or household activity’)  
In Case C-212/13,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Nejvyšší správní soud (Czech Republic), made by decision of 20 March 2013, received at the Court on 19 April 2013, in the proceedings  
František Ryneš  
v  
Úřad pro ochranu osobních údajů,  
THE COURT (Fourth Chamber),  
composed of L. Bay Larsen, President of the Chamber, K. Jürimäe, J. Malenovský, M. Safjan (Rapporteur) and A. Prechal, Judges,  
Advocate General: N. Jääskinen,  
Registrar: I. Illéssy, Administrator,  
having regard to the written procedure and further to the hearing on 20 March 2014,  
after considering the observations submitted on behalf of:  
–        Mr Ryneš, by M. Šalomoun, advokát,  
–        Úřad pro ochranu osobních údajů, by I. Němec, advokát, and J. Prokeš,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the Spanish Government, by A. Rubio González, acting as Agent,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by P. Gentili, avvocato dello Stato,  
–        the Austrian Government, by A. Posch and G. Kunnert, acting as Agents,  
–        the Polish Government, by B. Majczyna, J. Fałdyga and M. Kamejsza, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,  
–        the United Kingdom Government, by L. Christie, acting as Agent, and by J. Holmes, Barrister,  
–        the European Commission, by B. Martenczuk, P. Němečková and Z. Malůšková, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 10 July 2014,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 3(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Mr Ryneš and the Úřad pro ochranu osobních údajů (Office for Personal Data Protection; ‘the Office’), concerning a decision by which the Office found that Mr Ryneš had committed a number of offences in relation to the protection of personal data.  
   
Legal context  
   
EU law  
 Directive 95/46  
3        Recitals 10, 12 and 14 to 16 in the preamble to Directive 95/46 state:  
‘(10) … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; … for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;   
...  
(12)      … there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;   
...  
(14)  … given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;   
(15)  … the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;   
(16)      … the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law.’  
4        Under Article 2 of Directive 95/46:  
‘For the purposes of this Directive:   
(a)      “Personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference … to one or more factors specific to his physical … identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;   
(c)      “personal data filing system” (“filing system”) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;  
(d)       “controller” shall mean the natural … person … which alone or jointly with others determines the purposes and means of the processing of personal data ...’.  
5        Article 3 of that directive provides:   
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,   
–        by a natural person in the course of a purely personal or household activity.’  
6        Article 7 of Directive 95/46 is worded as follows:  
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent; or  
...  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for [sic] fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
7        Article 11 of Directive 95/46 provides:  
‘1.      Where the data have not been obtained from the data subject, Member States shall provide that the controller … must at the time of undertaking the recording of personal data … provide the data subject with at least the following information, except where he already has it:  
(a)      the identity of the controller ...;  
(b)      the purposes of the processing;  
(c)      any further information such as  
–        the categories of data concerned,  
–        the recipients or categories of recipients,  
–        the existence of the right of access to and the right to rectify the data concerning him  
insofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.  
2.      Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.  In these cases Member States shall provide appropriate safeguards.’  
8        Article 13(1) of the directive provides:  
‘Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Article … 11(1) … when such a restriction constitutes a necessary [measure] to safeguard:  
...  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
...  
(g)      the protection of … the rights and freedoms of others.’  
9        Under Article 18(1) of Directive 95/46:  
‘Member States shall provide that the controller … must notify the supervisory authority … before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.’  
   
Czech law  
10      Paragraph 3(3) of Law No 101/2000 Sb. on the Protection of Personal Data and the Amendment of Various Laws (‘Law No 101/2000’) provides:  
‘This Law does not cover the processing of personal data carried out by a natural person solely for personal use.’  
11      Paragraph 44(2) of that law governs the liability of the personal data controller, who commits an offence if he processes that data without the consent of the data subject, or if he does not provide the data subject with the relevant information or if he does not comply with the obligation to report to the competent authority.  
12      Under Paragraph 5(2)(e) of Law No 101/2000, the processing of personal data is in principle only possible with the consent of the data subject. In the absence of such consent, personal data may be processed where doing so is necessary to safeguard the legally protected rights and interests of the data controller, recipient or other data subjects. However, such processing must not adversely affect the data subject’s right to respect for his private and family life.  
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
13      During the period from 5 October 2007 to 11 April 2008, Mr Ryneš installed and used a camera system located under the eaves of his family home. The camera was installed in a fixed position and could not turn; it recorded the entrance to his home, the public footpath and the entrance to the house opposite. The system allowed only a visual recording, which was stored on recording equipment in the form of a continuous loop, that is to say, on a hard disk drive. As soon as it reached full capacity, the device would record over the existing recording, erasing the old material. No monitor was installed on the recording equipment, so the images could not be studied in real time. Only Mr Ryneš had direct access to the system and the data.  
14      The Nejvyšší správní soud (Supreme Administrative Court, Czech Republic; or ‘the referring court’) notes that Mr Ryneš’s only reason for operating the camera was to protect the property, health and life of his family and himself. Indeed, both Mr Ryneš and his family had for several years been subjected to attacks by persons unknown whom it had not been possible to identify. Furthermore, the windows of the family home had been broken on several occasions between 2005 and 2007.  
15      On the night of 6 to 7 October 2007, a further attack took place. One of the windows of Mr Ryneš’s home was broken by a shot from a catapult. The video surveillance system at issue made it possible to identify two suspects. The recording was handed over to the police and relied on in the course of the subsequent criminal proceedings.  
16      By decision of 4 August 2008, following a request from one of the suspects for confirmation that Mr Ryneš’s surveillance system was lawful, the Office found that Mr Ryneš had infringed Law No 101/2000, since:  
–        as a data controller, he had used a camera system to collect, without their consent, the personal data of persons moving along the street or entering the house opposite;  
–        he had not informed those persons of the processing of that personal data, the extent and purpose of that processing, by whom and by what means the personal data would be processed, or who would have access to the personal data; and  
–        as a data controller, Mr Ryneš had not fulfilled the obligation to report that processing to the Office.  
17      Mr Ryneš brought an action challenging that decision, which the Městský soud v Praze (Prague City Court) dismissed by judgment of 25 April 2012. Mr Ryneš brought an appeal on a point of law against that judgment before the referring court.  
18      In those circumstances, the Nejvyšší správní soud decided to stay proceedings and refer the following question to the Court of Justice for a preliminary ruling:  
‘Can the operation of a camera system installed on a family home for the purposes of the protection of the property, health and life of the owners of the home be classified as the processing of personal data “by a natural person in the course of a purely personal or household activity” for the purposes of Article 3(2) of Directive 95/46 …, even though such a system also monitors a public space?’  
   
Consideration of the question referred  
19      By its question, the referring court essentially asks whether, on a proper construction of the second indent of Article 3(2) of Directive 95/46, the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, amounts to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.  
20      It should be noted that, under Article 3(1) of Directive 95/46, the directive is to apply to ‘the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system’.  
21      The term ‘personal data’ as used in that provision covers, according to the definition under Article 2(a) of Directive 95/46, ‘any information relating to an identified or identifiable natural person’, an identifiable person being ‘one who can be identified, directly or indirectly, in particular by reference … to one or more factors specific to his physical … identity’.  
22      Accordingly, the image of a person recorded by a camera constitutes personal data within the meaning of Article 2(a) of Directive 95/46 inasmuch as it makes it possible to identify the person concerned.  
23      As regards the ‘processing of personal data’, it should be noted that Article 2(b) of Directive 95/46 defines this as ‘any operation or set of operations which is performed upon personal data, … such as collection, recording, … storage’.  
24      As can be seen, in particular, from recitals 15 and 16 to Directive 95/46, video surveillance falls, in principle, within the scope of that directive in so far as it constitutes automatic processing.  
25      Surveillance in the form of a video recording of persons, as in the case before the referring court, which is stored on a continuous recording device — the hard disk drive — constitutes, pursuant to Article 3(1) of Directive 95/46, the automatic processing of personal data.  
26      The referring court is uncertain whether such processing should nevertheless, in circumstances such as those of the case before it, escape the application of Directive 95/46 in so far as it is carried out ‘in the course of a purely personal or household activity’ for the purposes of the second indent of Article 3(2) of the directive.  
27      As is clear from Article 1 of that directive and recital 10 thereto, Directive 95/46 is intended to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (see   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 66).  
28      In that connection, it should be noted that, according to settled case-law, the protection of the fundamental right to private life guaranteed under Article 7 of the Charter of Fundamental Rights of the European Union (‘the Charter’) requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (see   
IPI  
, C-473/12, EU:C:2013:715, paragraph 39, and   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52).  
29      Since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter (see   
Google Spain and Google  
, EU:C:2014:317, paragraph 68), the exception provided for in the second indent of Article 3(2) of that directive must be narrowly construed.  
30      The fact that Article 3(2) of Directive 95/46 falls to be narrowly construed has its basis also in the very wording of that provision, under which the directive does not cover the processing of data where the activity in the course of which that processing is carried out is a ‘purely’ personal or household activity, that is to say, not simply a personal or household activity.  
31      In the light of the foregoing considerations, it must be held that, as the Advocate General observed in point 53 of his Opinion, the processing of personal data comes within the exception provided for in the second indent of Article 3(2) of Directive 95/46 only where it is carried out in the purely personal or household setting of the person processing the data.  
32      Accordingly, so far as natural persons are concerned, correspondence and the keeping of address books constitute, in the light of recital 12 to Directive 95/46, a ‘purely personal or household activity’ even if they incidentally concern or may concern the private life of other persons.  
33      To the extent that video surveillance such as that at issue in the main proceedings covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely ‘personal or household’ activity for the purposes of the second indent of Article 3(2) of Directive 95/46.  
34      At the same time, the application of Directive 95/46 makes it possible, where appropriate, to take into account — in accordance, in particular, with Articles 7(f), 11(2), and 13(1)(d) and (g) of that directive — legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the case in the main proceedings.  
35      Consequently, the answer to the question referred is that the second indent of Article 3(2) of Directive 95/46 must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.  
   
Costs  
36      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Fourth Chamber) hereby rules:  
The second indent of Article 3(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.

ID: 43a740e9-a032-432c-9090-d9f25a9f283c

Judgment of 24 Sep 2019, C-136/17 (  
GC and Others  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Special categories of personal data   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to object   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Special categories of personal data   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
   
JUDGMENT OF THE COURT (Grand Chamber)  
24 September 2019 (\*)  
(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of personal data contained on websites — Directive 95/46/EC — Regulation (EU) 2016/679 — Search engines on the internet — Processing of data appearing on websites — Special categories of data referred to in Article 8 of Directive 95/46 and Articles 9 and 10 of Regulation 2016/679 — Applicability of those articles to operators of a search engine — Extent of that operator’s obligations with respect to those articles — Publication of data on websites solely for journalistic purposes or the purpose of artistic or literary expression — Effect on the handling of a request for de-referencing — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)  
In Case C-136/17,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Conseil d’État (Council of State, France), made by decision of 24 February 2017, received at the Court on 15 March 2017, in the proceedings  
GC,  
AF,  
BH,  
ED  
v  
Commission nationale de l’informatique et des libertés (CNIL),  
interveners:  
Premier ministre,  
Google LLC,   
 successor to Google Inc.,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, T. von Danwitz, C. Toader and F. Biltgen, Presidents of Chambers, M. Ilešič (Rapporteur), L. Bay Larsen, M. Safjan, D. Šváby, C.G. Fernlund, C. Vajda and S. Rodin, Judges,  
Advocate General: M. Szpunar,  
Registrar: V. Giacobbo-Peyronnel, administrator,  
having regard to the written procedure and further to the hearing on 11 September 2018,  
after considering the observations submitted on behalf of:  
–        AF, by himself,  
–        BH, by L. Boré, avocat,  
–        Commission nationale de l’informatique et des libertés (CNIL), by I. Falque-Pierrotin, J. Lessi and G. Le Grand, acting as Agents,  
–        Google LLC, by P. Spinosi, Y. Pelosi and W. Maxwell, avocats,  
–        the French Government, by D. Colas, R. Coesme, E. de Moustier and S. Ghiandoni, acting as Agents,  
–        Ireland, by M. Browne, G. Hodge, J. Quaney and A. Joyce, acting as Agents, and M. Gray, Barrister-at-Law,  
–        the Greek Government, by E.-M. Mamouna, G. Papadaki, E. Zisi and S. Papaioannou, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and F. De Luca and P. Gentili, avvocati dello Stato,  
–        the Austrian Government, by G. Eberhard and G. Kunnert, acting as Agents,  
–        the Polish Government, by B. Majczyna, M. Pawlicka and J. Sawicka, acting as Agents,  
–        the United Kingdom Government, by S. Brandon, acting as Agent, and C. Knight, Barrister,  
–        the European Commission, by A. Buchet, H. Kranenborg and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 10 January 2019,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between GC, AF, BH and ED and the Commission nationale de l’informatique et des libertés (French Data Protection Authority, France) (‘the CNIL’) concerning four decisions of the CNIL refusing to serve formal notice on Google Inc., now Google LLC, to de-reference various links appearing in the lists of results displayed following searches of their names and leading to web pages published by third parties.  
   
Legal context  
   
EU law  
   
Directive 95/46  
3        The object of Directive 95/46, in accordance with Article 1(1), is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and to eliminate obstacles to the free flow of personal data.  
4        Recitals 33 and 34 of Directive 95/46 state:  
‘(33)      Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs …  
(34)      Whereas Member States must also be authorised, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data …; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;’  
5        Article 2 of Directive 95/46 provides:  
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); …  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; …  
…  
(h)      “the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.’  
6        In Chapter II, Section I of Directive 95/46, headed ‘Principles relating to data quality’, Article 6 reads as follows:  
‘1.      Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. …  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
7        In Chapter II, Section II of Directive 95/46, headed ‘Criteria for making data processing legitimate’, Article 7 provides:  
‘Member States shall provide that personal data may be processed only if:  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
8        Articles 8 and 9 of Directive 95/46 appear in Chapter II, Section III, headed ‘Special categories of processing’. Article 8, headed ‘The processing of special categories of data’, provides:  
‘1.      Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.  
2.      Paragraph 1 shall not apply where:  
(a)      the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject’s giving his consent; or  
…  
(e)      the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.  
…  
4.      Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.  
5.      Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.  
Member States may provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of official authority.  
…’  
9        Article 9 of Directive 95/46, headed ‘Processing of personal data and freedom of expression’, states:  
‘Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.’  
10      Article 12 of Directive 95/46, headed ‘Right of access’, provides:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
…  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
…’  
11      Article 14 of Directive 95/46, headed ‘The data subject’s right to object’, provides:  
‘Member States shall grant the data subject the right:  
(a)      at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;  
…’  
12      Article 28 of Directive 95/46, headed ‘Supervisory authority’, reads as follows:  
‘1.      Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.  
…  
3.      Each authority shall in particular be endowed with:  
–        investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,  
–        effective powers of intervention, such as, for example, that … of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing …  
–        …  
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.  
4.      Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.  
…  
6.      Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.  
The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.  
…’  
   
Regulation (EU) 2016/679  
13      Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2) applies, in accordance with Article 99(2), from 25 May 2018. Article 94(1) of that regulation provides that Directive 95/46 is repealed with effect from that date.  
14      Recitals 1, 4, 51, 52 and 65 of Regulation 2016/679 state:  
‘(1)      The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the “Charter”) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.  
…  
(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, … the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, …  
…  
(51)      Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. …  
(52)      Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights …  
…  
(65)      A data subject should have … a “right to be forgotten” where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. … However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information …’  
15      Article 4(11) of Regulation 2016/679 defines ‘consent’ as ‘any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.  
16      Article 5 of Regulation 2016/679, headed ‘Principles relating to processing of personal data’, provides in paragraph 1(c) to (e):  
‘Personal data shall be:  
…  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; … (“storage limitation”).’  
17      Article 9 of Regulation 2016/679, headed ‘Processing of special categories of personal data’, provides:  
‘1.      Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.  
2.      Paragraph 1 shall not apply if one of the following applies:  
(a)      the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;  
…  
(e)      processing relates to personal data which are manifestly made public by the data subject;  
…  
(g)      processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;  
…’  
18      Article 10 of Regulation 2016/679, headed ‘Processing of personal data relating to criminal convictions and offences’, provides:  
‘Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.’  
19      Article 17 of Regulation 2016/679, headed ‘Right to erasure (“right to be forgotten”)’, reads as follows:  
‘1.      The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:  
(a)      the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;  
(b)      the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;  
(c)      the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);  
(d)      the personal data have been unlawfully processed;  
(e)      the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;  
(f)      the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).  
2.      Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.  
3.      Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:  
(a)      for exercising the right of freedom of expression and information;  
…’  
20      Article 21 of Regulation 2016/679, headed ‘Right to object’, provides in paragraph 1:  
‘The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.’  
21      Article 85 of Regulation 2016/679, headed ‘Processing and freedom of expression and information’, provides:  
‘1.      Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.  
2.      For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.  
…’  
   
French law  
22      Directive 95/46 was implemented in French law by Loi No 78-17, du 6 janvier 1978, relative à l’informatique, aux fichiers et aux libertés (Law No 78-17 of 6 January 1978 on information technology, data files and civil liberties), in the version applicable to the facts of the main proceedings.  
23      Article 11 of that law states that, among its functions, the CNIL is to ensure that the processing of personal data is carried out in accordance with the provisions of that law, and that, on that basis, it is to receive claims, petitions and complaints relating to the processing of personal data and is to inform their authors of their outcome.  
   
The disputes in the main proceedings and the questions referred for a preliminary ruling  
24      GC, AF, BH and ED each requested Google to de-reference, in the list of results displayed by the search engine operated by Google in response to searches against their names, various links leading to web pages published by third parties; Google, however, refused to do this.  
25      More particularly, GC requested the de-referencing of a link leading to a satirical photomontage placed online pseudonymously on 18 February 2011 on YouTube, depicting her alongside the mayor of a municipality whom she served as head of cabinet and explicitly referring to an intimate relationship between them and to the impact of that relationship on her own political career. The photomontage was placed online during the campaign for the cantonal elections in which GC was then a candidate. On the date on which her request for de-referencing was refused she was neither a local councillor nor a candidate for local elective office and no longer served as the head of cabinet of the mayor of the municipality.  
26      AF requested de-referencing of links leading to an article in the daily newspaper   
Libération  
 of 9 September 2008, reproduced on the site of the Centre contre les manipulations mentales (Centre against mental manipulation) (CCMM) (France), concerning the suicide of a member of the Church of Scientology in December 2006. AF is mentioned in that article in his capacity as public relations officer of the Church of Scientology, an occupation which he has since ceased to exercise. Furthermore, the author of the article states that he contacted AF in order to obtain his version of the facts and describes the comments received on that occasion.  
27      BH requested the de-referencing of links leading to articles, mainly in the press, concerning the judicial investigation opened in June 1995 into the funding of the Parti républicain (PR), in which he was questioned with a number of businessmen and political personalities. The proceedings against him were closed by an order discharging him on 26 February 2010. Most of the links are to articles contemporaneous with the opening of the investigation and therefore do not mention the outcome of the proceedings.  
28      ED requested the de-referencing of links leading to two articles published in   
Nice Matin  
 and   
Le Figaro  
 reporting the criminal hearing during which he was sentenced to 7 years’ imprisonment and an additional penalty of 10 years’ social and judicial supervision for sexual assaults on children under the age of 15. One of the accounts of the court proceedings also mentions several intimate details relating to ED that were revealed at the hearing.  
29      Following the rejections by Google of their requests for de-referencing, the applicants in the main proceedings brought complaints before the CNIL, seeking for Google to be ordered to de-reference the links in question. By letters dated 24 April 2015, 28 August 2015, 21 March 2016 and 9 May 2016 respectively, the president of the CNIL informed them that the procedures on their complaints had been closed.  
30      The applicants in the main proceedings thereupon made applications to the referring court, the Conseil d’État (Council of State, France), against those refusals of the CNIL to serve formal notice on Google to carry out the de-referencing requested. The applications were joined by the referring court.  
31      Finding that the applications raised several serious difficulties of interpretation of Directive 95/46, the Conseil d’État (Council of State) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Having regard to the specific responsibilities, powers and capabilities of the operator of a search engine, does the prohibition imposed on other controllers of processing data caught by Article 8(1) and (5) of Directive 95/46, subject to the exceptions laid down there, also apply to this operator as the controller of processing by means of that search engine?  
(2)      If Question 1 should be answered in the affirmative:  
[(a)]      Must Article 8(1) and (5) of Directive 95/46 be interpreted as meaning that the prohibition so imposed on the operator of a search engine of processing data covered by those provisions, subject to the exceptions laid down by that directive, would require the operator to grant as a matter of course the requests for de-referencing in relation to links to web pages concerning such data?  
[(b)]      From that perspective, how must the exceptions laid down in Article 8(2)(a) and (e) of Directive 95/46 be interpreted, when they apply to the operator of a search engine, in the light of its specific responsibilities, powers and capabilities? In particular, may such an operator refuse a request for de-referencing, if it establishes that the links at issue lead to content which, although comprising data falling within the categories listed in Article 8(1), is also covered by the exceptions laid down by Article 8(2) of the directive, in particular points (a) and (e)?  
[(c)]      Similarly, when the links subject to the request for de-referencing lead to processing of personal data carried out solely for journalistic purposes or for those of artistic or literary expression, on which basis, in accordance with Article 9 of Directive 95/46, data within the categories mentioned in Article 8(1) and (5) of the directive may be collected and processed, must the provisions of Directive 95/46 be interpreted as allowing the operator of a search engine, on that ground, to refuse a request for de-referencing?  
(3)      If Question 1 should be answered in the negative:  
[(a)]      Which specific requirements of Directive 95/46 must be met by the operator of a search engine, in view of its responsibilities, powers and capabilities?  
[(b)]      When the operator establishes that the web pages at the end of the links subject to the request for de-referencing comprise data whose publication on those pages is unlawful, must the provisions of Directive 95/46 be interpreted as:  
–        requiring the operator of a search engine to remove those links from the list of results displayed following a search made on the basis of the name of the person making the request; or  
–        meaning only that it is to take that factor into consideration in assessing the merits of the request for de-referencing, or  
–        meaning that this factor has no bearing on the assessment it is to make?  
Furthermore, if that factor is not irrelevant, how is the lawfulness of the publication on web pages of the data at issue which stem from processing falling outside the territorial scope of Directive 95/46 and, accordingly, of the national laws implementing it to be assessed?  
(4)      Irrespective of the answer to be given to Question 1:  
[(a)]      whether or not publication of the personal data on the web page at the end of the link at issue is lawful, must the provisions of Directive 95/46 be interpreted as:  
–        requiring the operator of a search engine, when the person making the request establishes that the data in question have become incomplete or inaccurate, or are no longer up to date, to grant the corresponding request for de-referencing;  
–        more specifically, requiring the operator of a search engine, when the person making the request shows that, having regard to the conduct of the legal proceedings, the information relating to an earlier stage of those proceedings is no longer consistent with the current reality of his situation, to de-reference the links to web pages comprising such information?  
[(b)]      Must Article 8(5) of Directive 95/46 be interpreted as meaning that information relating to the investigation of an individual or reporting a trial and the resulting conviction and sentencing constitutes data relating to offences and to criminal convictions? More generally, does a web page comprising data referring to the convictions of or legal proceedings involving a natural person fall within the ambit of those provisions?’  
   
Consideration of the questions referred  
32      The questions referred concern the interpretation of Directive 95/46, which was applicable at the time when the request for a preliminary ruling was submitted. That directive was repealed with effect from 25 May 2018, from which date Regulation 2016/679 applies.  
33      The Court will consider the questions referred from the point of view of Directive 95/46, while also taking Regulation 2016/679 into account in its analysis of them, in order to ensure that its answers will in any event be of use to the referring court.  
   
Q  
uestion  
 1  
34      By its first question, the referring court essentially asks whether the provisions of Article 8(1) and (5) of Directive 95/46 must be interpreted as meaning that the prohibition or restrictions relating to the processing of special categories of personal data, mentioned in those provisions, apply also, subject to the exceptions provided for by the directive, to the operator of a search engine in the context of his responsibilities, powers and capabilities as the controller of the processing carried out for the needs of the functioning of the search engine.  
35      It must be recalled, first, that the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of Article 2(b) of Directive 95/46 when that information contains personal data and, second, that the operator of the search engine must be regarded as the ‘controller’ in respect of that processing within the meaning of Article 2(d) of that directive (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 41).  
36      The processing of personal data in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page, and that activity plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject’s name, including to internet users who otherwise would not have found the web page on which those data are published. Moreover, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users’ access to that information may, when users carry out their search on the basis of an individual’s name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet, enabling them to establish a more or less detailed profile of the data subject (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraphs 35 to 37).  
37      Consequently, in so far as the activity of a search engine is liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of his responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 38).  
38      The first question referred aims to determine whether, in the context of his responsibilities, powers and capabilities, the operator of a search engine must also comply with the requirements laid down by Directive 95/46 with respect to the special categories of personal data mentioned in Article 8(1) and (5) of the directive, where such data are among the information published or placed on the internet by third parties and are the subject of processing by that operator for the purposes of the functioning of his search engine.  
39      As regards the special categories of data, Article 8(1) of Directive 95/46 provides that the Member States are to prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of data concerning health or sex life. Certain exceptions to and derogations from that prohibition are provided for inter alia in Article 8(2) of the directive.  
40      Article 8(5) of Directive 95/46 states that the processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgments in civil cases are also to be processed under the control of official authority.  
41      The content of Article 8(1) and (5) of Directive 95/46 was taken over, with some changes, in Article 9(1) and Article 10 of Regulation 2016/679.  
42      It must be stated, first, that it is apparent from the wording of those provisions of Directive 95/46 and Regulation 2016/679 that the prohibition and restrictions laid down by them apply, subject to the exceptions provided for by the directive and the regulation, to every kind of processing of the special categories of data referred to in those provisions and to all controllers carrying out such processing.  
43      Next, no other provision of that directive or that regulation provides for a general derogation from that prohibition or those restrictions for processing such as that carried out in the context of the activity of a search engine. On the contrary, as already pointed out in paragraph 37 above, it follows from the general scheme of those instruments that the operator of a search engine must, in the same way as any other controller, ensure, in the context of his responsibilities, powers and capabilities, that the processing of personal data carried out by him complies with the respective requirements of Directive 95/46 or Regulation 2016/679.  
44      Finally, an interpretation of Article 8(1) and (5) of Directive 95/46 or Article 9(1) and Article 10 of Regulation 2016/679 that excluded a priori and generally the activity of a search engine from the specific requirements laid down by those provisions for processing relating to the special categories of data referred to there would run counter to the purpose of those provisions, namely to ensure enhanced protection as regards such processing, which, because of the particular sensitivity of the data, is liable to constitute, as also follows from recital 33 of that directive and recital 51 of that regulation, a particularly serious interference with the fundamental rights to privacy and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter.  
45      While, contrary to the submissions of Google in particular, the specific features of the processing carried out by the operator of a search engine in connection with the activity of the search engine cannot thus justify the operator being exempted from compliance with Article 8(1) and (5) of Directive 95/46 and Article 9(1) and Article 10 of Regulation 2016/679, those specific features may, however, have an effect on the extent of the operator’s responsibility and obligations under those provisions.  
46      It must be observed in this respect that, as the European Commission emphasises, the operator of a search engine is responsible not because personal data referred to in those provisions appear on a web page published by a third party but because of the referencing of that page and in particular the display of the link to that web page in the list of results presented to internet users following a search on the basis of an individual’s name, since such a display of the link in such a list is liable significantly to affect the data subject’s fundamental rights to privacy and to the protection of the personal data relating to him (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 80).  
47      In those circumstances, having regard to the responsibilities, powers and capabilities of the operator of a search engine as the controller of the processing carried out in connection with the activity of the search engine, the prohibitions and restrictions in Article 8(1) and (5) of Directive 95/46 and Articles 9(1) and 10 of Regulation 2016/679 — as indicated by the Advocate General in point 56 of his Opinion and as stated in essence by all the parties who have expressed an opinion on the point — can apply to that operator only by reason of that referencing and thus via a verification, under the supervision of the competent national authorities, on the basis of a request by the data subject.  
48      It follows from the above that the answer to Question 1 is that the provisions of Article 8(1) and (5) of Directive 95/46 must be interpreted as meaning that the prohibition or restrictions relating to the processing of special categories of personal data, mentioned in those provisions, apply also, subject to the exceptions provided for by the directive, to the operator of a search engine in the context of his responsibilities, powers and capabilities as the controller of the processing carried out in connection with the activity of the search engine, on the occasion of a verification performed by that operator, under the supervision of the competent national authorities, following a request by the data subject.  
   
Q  
uestion  
 2  
49      By its second question, which consists of three parts, the referring court essentially asks  
–        whether the provisions of Article 8(1) and (5) of Directive 95/46 must be interpreted as meaning that the operator of a search engine is required by those provisions, subject to the exceptions provided for by the directive, to accede to requests for de-referencing in relation to links to web pages containing personal data falling within the special categories referred to by those provisions;  
–        whether Article 8(2)(a) and (e) of Directive 95/46 must be interpreted as meaning that, pursuant to that article, such an operator may refuse to accede to a request for de-referencing if he establishes that the links at issue lead to content comprising personal data falling within the special categories referred to in Article 8(1) but whose processing is covered by one of the exceptions laid down in Article 8(2)(a) and (e) of the directive; and  
–        whether the provisions of Directive 95/46 must be interpreted as meaning that the operator of a search engine may also refuse to accede to a request for de-referencing on the ground that the links whose de-referencing is requested lead to web pages on which the personal data falling within the special categories referred to in Article 8(1) or (5) of the directive are published solely for journalistic purposes or those of artistic or literary expression and the publication is therefore covered by the exception in Article 9 of the directive.  
50      It should be noted, as a preliminary point, that in the context of Directive 95/46 requests for de-referencing such as those at issue in the main proceedings have their basis in particular in Article 12(b) of the directive, under which the Member States are to guarantee data subjects the right to obtain from the controller the erasure of data whose processing does not comply with the directive.  
51      Moreover, in accordance with Article 14(a) of Directive 95/46, the Member States are to grant the data subject the right, at least in the cases referred to in Article 7(e) and (f) of the directive, to object at any time on compelling legitimate grounds relating to his or her particular situation to the processing of data relating to him or her, save where otherwise provided by national legislation.  
52      In this respect, it must be recalled that the Court has held that Article 12(b) and Article 14(a) of Directive 95/46 must be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 88).  
53      The Court has also held that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him or her personally should, at the present point in time, no longer be linked to his or her name by a list of results displayed following a search made on the basis of his or her name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his or her fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject’s name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his or her fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 99).  
54      With respect to Regulation 2016/679, the EU legislature laid down, in Article 17 of the regulation, a provision specifically governing the ‘right to erasure’, also called the ‘right to be forgotten’ in the heading of that article.  
55      In accordance with Article 17(1) of the regulation, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase those data without undue delay where one of the grounds set out in that provision applies. As grounds, the provision mentions the cases in which the personal data are no longer necessary in relation to the purposes for which they were processed; the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing; the data subject objects to the processing pursuant to Article 21(1) or (2) of the regulation, which replaces Article 14 of Directive 95/46; the data have been unlawfully processed; the data have to be erased for compliance with a legal obligation; or the data have been collected in relation to the offer of information society services to children.  
56      However, Article 17(3) of Regulation 2016/679 states that Article 17(1) of the regulation is not to apply to the extent that the processing is necessary on one of the grounds set out in Article 17(3). Among those grounds is, in Article 17(3)(a) of the regulation, the exercise of the right of freedom of expression and information.  
57      The circumstance that Article 17(3)(a) of Regulation 2016/679 now expressly provides that the data subject’s right to erasure is excluded where the processing is necessary for the exercise of the right of information, guaranteed by Article 11 of the Charter, is an expression of the fact that the right to protection of personal data is not an absolute right but, as recital 4 of the regulation states, must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality (see also judgment of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48, and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 136).  
58      In that context, it should be recalled that Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 50).  
59      Regulation 2016/679, in particular Article 17(3)(a), thus expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter, on the one hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other.  
60      It is in the light of those considerations that an examination must be made of the conditions in which the operator of a search engine is required to accede to a request for de-referencing and thus to delete from the list of results displayed following a search on the basis of the data subject’s name the link to a web page on which there are personal data falling within the special categories in Article 8(1) and (5) of Directive 95/46.  
61      It must be stated, to begin with, that the processing by the operator of a search engine of the special categories of data referred to in Article 8(1) of Directive 95/46 is capable in principle of being covered by the exceptions in Article 8(2)(a) and (e), mentioned by the referring court, which provides that the prohibition is not to apply where the data subject has given his or her explicit consent to such processing, except where the laws of the Member State concerned prohibit such consent, or where the processing relates to data which are manifestly made public by the data subject. Those exceptions have now been repeated in Article 9(2)(a) and (e) of Regulation 2016/679. In addition, Article 9(2)(g) of the regulation, which essentially reproduces Article 8(4) of Directive 95/46, allows the processing of those categories of data where it is necessary for reasons of substantial public interest, on the basis of European Union or Member State law which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.  
62      With respect to the exception in Article 8(2)(a) of Directive 95/46 and Article 9(2)(a) of Regulation 2016/679, it follows from the definition of ‘consent’ in Article 2(h) of that directive and Article 4(11) of that regulation that the consent must be ‘specific’ and must therefore relate specifically to the processing carried out in connection with the activity of the search engine, and thus to the fact that the processing enables third parties, by means of a search based on the data subject’s name, to obtain a list of results including links leading to web pages containing sensitive data relating to him or her. In practice, it is scarcely conceivable — nor, moreover, does it appear from the documents before the Court — that the operator of a search engine will seek the express consent of data subjects before processing personal data concerning them for the purposes of his referencing activity. In any event, as inter alia the French and Polish Governments and the Commission have observed, the mere fact that a person makes a request for de-referencing means, in principle, at least at the time of making the request, that he or she no longer consents to the processing carried out by the operator of the search engine. In this connection, it should also be recalled that Article 17(1)(b) of the regulation mentions among the grounds justifying the ‘right to be forgotten’ the data subject’s withdrawal of the consent on which the processing is based in accordance with Article 9(2)(a) of the regulation, where there is no other legal ground for the processing.  
63      By contrast, the circumstance, referred to in Article 8(2)(e) of Directive 95/46 and Article 9(2)(e) of Regulation 2016/679, that the data in question are manifestly made public by the data subject is intended to apply, as has been observed by all those who have made submissions on the point, both to the operator of the search engine and to the publisher of the web page concerned.  
64      Consequently, in such a case, despite the presence on the web page referenced of personal data falling within the special categories in Article 8(1) of Directive 95/46 and Article 9(1) of Regulation 2016/679, the processing of those data by the operator of the search engine in connection with its activity, provided that the other conditions of lawfulness are satisfied, in particular those laid down by Article 6 of the directive or Article 5 of the regulation (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 72), is compliant with those provisions.  
65      However, even in that case, the data subject may, pursuant to Article 14(a) of Directive 95/46 or Article 17(1)(c) and Article 21(1) of Regulation 2016/679, have the right to de-referencing of the link in question on grounds relating to his or her particular situation.  
66      In any event, when the operator of a search engine receives a request for de-referencing, he must ascertain, having regard to the reasons of substantial public interest referred to in Article 8(4) of Directive 95/46 or Article 9(2)(g) of Regulation 2016/679 and in compliance with the conditions laid down in those provisions, whether the inclusion of the link to the web page in question in the list displayed following a search on the basis of the data subject’s name is necessary for exercising the right of freedom of information of internet users potentially interested in accessing that web page by means of such a search, a right protected by Article 11 of the Charter. While the data subject’s rights protected by Articles 7 and 8 of the Charter override, as a general rule, the freedom of information of internet users, that balance may, however, depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject’s private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 81).  
67      Furthermore, where the processing relates to the special categories of data mentioned in Article 8(1) and (5) of Directive 95/46 or Article 9(1) and Article 10 of Regulation 2016/679, the interference with the data subject’s fundamental rights to privacy and protection of personal data is, as observed in paragraph 44 above, liable to be particularly serious because of the sensitivity of those data.  
68      Consequently, where the operator of a search engine receives a request for de-referencing relating to a link to a web page on which such sensitive data are published, the operator must, on the basis of all the relevant factors of the particular case and taking into account the seriousness of the interference with the data subject’s fundamental rights to privacy and protection of personal data laid down in Articles 7 and 8 of the Charter, ascertain, having regard to the reasons of substantial public interest referred to in Article 8(4) of Directive 95/46 or Article 9(2)(g) of Regulation 2016/679 and in compliance with the conditions laid down in those provisions, whether the inclusion of that link in the list of results displayed following a search on the basis of the data subject’s name is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the Charter.  
69      It follows from all the above considerations that the answer to Question 2 is as follows:  
–        The provisions of Article 8(1) and (5) of Directive 95/46 must be interpreted as meaning that the operator of a search engine is in principle required by those provisions, subject to the exceptions provided for by the directive, to accede to requests for de-referencing in relation to links to web pages containing personal data falling within the special categories referred to by those provisions.  
–        Article 8(2)(e) of Directive 95/46 must be interpreted as meaning that, pursuant to that article, such an operator may refuse to accede to a request for de-referencing if he establishes that the links at issue lead to content comprising personal data falling within the special categories referred to in Article 8(1) but whose processing is covered by the exception in Article 8(2)(e) of the directive, provided that the processing satisfies all the other conditions of lawfulness laid down by the directive, and unless the data subject has the right under Article 14(a) of the directive to object to that processing on compelling legitimate grounds relating to his particular situation.  
–        The provisions of Directive 95/46 must be interpreted as meaning that, where the operator of a search engine has received a request for de-referencing relating to a link to a web page on which personal data falling within the special categories referred to in Article 8(1) or (5) of Directive 95/46 are published, the operator must, on the basis of all the relevant factors of the particular case and taking into account the seriousness of the interference with the data subject’s fundamental rights to privacy and protection of personal data laid down in Articles 7 and 8 of the Charter, ascertain, having regard to the reasons of substantial public interest referred to in Article 8(4) of the directive and in compliance with the conditions laid down in that provision, whether the inclusion of that link in the list of results displayed following a search on the basis of the data subject’s name is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the Charter.  
   
Q  
uestion  
 3  
70      As this question is asked only in the event that Question 1 is answered in the negative, there is no need to answer it, given the affirmative answer to Question 1.  
   
Q  
uestion  
 4  
71      By its fourth question, the referring court essentially asks whether the provisions of Directive 95/46 must be interpreted as meaning that  
–        first, information relating to legal proceedings brought against an individual and, as the case may be, information relating to an ensuing conviction are data relating to ‘offences’ and ‘criminal convictions’ within the meaning of Article 8(5) of Directive 95/46, and  
–        second, the operator of a search engine is required to accede to a request for de-referencing relating to links to web pages displaying such information, where the information relates to an earlier stage of the legal proceedings in question and, having regard to the progress of the proceedings, no longer corresponds to the current situation?  
72      In this respect, it must be stated, as the Advocate General observed in point 100 of his Opinion and as submitted inter alia by the French Government, Ireland, the Italian and Polish Governments and the Commission, that information concerning legal proceedings brought against an individual, such as information relating to the judicial investigation and the trial and, as the case may be, the ensuing conviction, is data relating to ‘offences’ and ‘criminal convictions’ within the meaning of the first subparagraph of Article 8(5) of Directive 95/46 and Article 10 of Regulation 2016/679, regardless of whether or not, in the course of those legal proceedings, the offence for which the individual was prosecuted was shown to have been committed.  
73      Consequently, by including in the list of results displayed following a search carried out on the basis of the data subject’s name links to web pages on which such data are published, the operator of a search engine carries out a processing of those data which, in accordance with the first subparagraph of Article 8(5) of Directive 95/46 and Article 10 of Regulation 2016/679, is subject to special restrictions. As the Commission observed, such processing may, by virtue of those provisions and subject to compliance with the other conditions of lawfulness laid down by that directive, be lawful in particular if appropriate and specific guarantees are provided for by national law, which may be the case where the information in question has been disclosed to the public by the public authorities in compliance with the applicable national law.  
74      As regards those other conditions of lawfulness, it must be recalled that it follows from the requirements laid down in Article 6(1)(c) to (e) of Directive 95/46, now repeated in Article 5(1)(c) to (e) of Regulation 2016/679, that even initially lawful processing of accurate data may over time become incompatible with the directive or the regulation where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 93).  
75      However, as stated in paragraph 66 above, even if the processing of data referred to in Article 8(5) of Directive 95/46 and Article 10 of Regulation 2016/679 does not correspond to the restrictions laid down by those provisions or the other conditions of lawfulness, such as those laid down in Article 6(1)(c) to (e) of the directive and Article 5(1)(c) to (e) of the regulation, the operator of a search engine must still ascertain, having regard to the reasons of substantial public interest referred to in Article 8(4) of the directive or Article 9(2)(g) of the regulation and in compliance with the conditions laid down in those provisions, whether the inclusion of the link to the web page in question in the list displayed following a search on the basis of the data subject’s name is necessary for exercising the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the Charter.  
76      In this respect, it must be recalled that it follows from the case-law of the European Court of Human Rights that applications brought by individuals for the prohibition under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950, of the making available on the internet by the various media of old reports of criminal proceedings that had been brought against them call for an examination of the fair balance to be struck between their right to respect for their private life and inter alia the public’s freedom of information. In seeking that fair balance, account must be taken of the essential role played by the press in a democratic society, which includes reporting and commenting on legal proceedings. Moreover, to the media’s function of communicating such information and ideas there must be added the public’s right to receive them. The European Court of Human Rights acknowledged in this context that the public had an interest not only in being informed about a topical event, but also in being able to conduct research into past events, with the public’s interest as regards criminal proceedings varying in degree, however, and possibly evolving over time according in particular to the circumstances of the case (ECtHR, 28 June 2018,   
M.L. and W.W. v. Germany  
, CE:ECHR:2018:0628JUD006079810, §§ 89 and 100 to 102).  
77      It is thus for the operator of a search engine to assess, in the context of a request for de-referencing relating to links to web pages on which information is published relating to criminal proceedings brought against the data subject, concerning an earlier stage of the proceedings and no longer corresponding to the current situation, whether, in the light of all the circumstances of the case, such as, in particular, the nature and seriousness of the offence in question, the progress and the outcome of the proceedings, the time elapsed, the part played by the data subject in public life and his past conduct, the public’s interest at the time of the request, the content and form of the publication and the consequences of publication for the data subject, he or she has a right to the information in question no longer, in the present state of things, being linked with his or her name by a list of results displayed following a search carried out on the basis of that name.  
78      It must, however, be added that, even if the operator of a search engine were to find that that is not the case because the inclusion of the link in question is strictly necessary for reconciling the data subject’s rights to privacy and protection of personal data with the freedom of information of potentially interested internet users, the operator is in any event required, at the latest on the occasion of the request for de-referencing, to adjust the list of results in such a way that the overall picture it gives the internet user reflects the current legal position, which means in particular that links to web pages containing information on that point must appear in first place on the list.  
79      Having regard to the above considerations, the answer to Question 4 is that the provisions of Directive 95/46 must be interpreted as meaning that  
–        first, information relating to legal proceedings brought against an individual and, as the case may be, information relating to an ensuing conviction are data relating to ‘offences’ and ‘criminal convictions’ within the meaning of Article 8(5) of Directive 95/46, and  
–        second, the operator of a search engine is required to accede to a request for de-referencing relating to links to web pages displaying such information, where the information relates to an earlier stage of the legal proceedings in question and, having regard to the progress of the proceedings, no longer corresponds to the current situation, in so far as it is established in the verification of the reasons of substantial public interest referred to in Article 8(4) of Directive 95/46 that, in the light of all the circumstances of the case, the data subject’s fundamental rights guaranteed by Articles 7 and 8 of the Charter override the rights of potentially interested internet users protected by Article 11 of the Charter.  
   
Costs  
80      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
The provisions of Article 8(1) and (5) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the prohibition or restrictions relating to the processing of special categories of personal data, mentioned in those provisions, apply also, subject to the exceptions provided for by the directive, to the operator of a search engine in the context of his responsibilities, powers and capabilities as the controller of the processing carried out in connection with the activity of the search engine, on the occasion of a verification performed by that operator, under the supervision of the competent national authorities, following a request by the data subject.  
2.        
The provisions of Article 8(1) and (5) of Directive 95/46 must be interpreted as meaning that the operator of a search engine is in principle required by those provisions, subject to the exceptions provided for by the directive, to accede to requests for de-referencing in relation to links to web pages containing personal data falling within the special categories referred to by those provisions.  
Article 8(2)(e) of Directive 95/46 must be interpreted as meaning that, pursuant to that article, such an operator may refuse to accede to a request for de-referencing if he establishes that the links at issue lead to content comprising personal data falling within the special categories referred to in Article 8(1) but whose processing is covered by the exception in Article 8(2)(e) of the directive, provided that the processing satisfies all the other conditions of lawfulness laid down by the directive, and unless the data subject has the right under Article 14(a) of the directive to object to that processing on compelling legitimate grounds relating to his particular situation.  
The provisions of Directive 95/46 must be interpreted as meaning that, where the operator of a search engine has received a request for de-referencing relating to a link to a web page on which personal data falling within the special categories referred to in Article 8(1) or (5) of Directive 95/46 are published, the operator must, on the basis of all the relevant factors of the particular case and taking into account the seriousness of the interference with the data subject’s fundamental rights to privacy and protection of personal data laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, ascertain, having regard to the reasons of substantial public interest referred to in Article 8(4) of the directive and in compliance with the conditions laid down in that provision, whether the inclusion of that link in the list of results displayed following a search on the basis of the data subject’s name is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the Charter.  
3.        
The provisions of Directive 95/46 must be interpreted as meaning that  
–          
first, information relating to legal proceedings brought against an individual and, as the case may be, information relating to an ensuing conviction are data relating to ‘offences’ and ‘criminal convictions’ within the meaning of Article 8(5) of Directive 95/46, and  
–          
second, the operator of a search engine is required to accede to a request for de-referencing relating to links to web pages displaying such information, where the information relates to an earlier stage of the legal proceedings in question and, having regard to the progress of the proceedings, no longer corresponds to the current situation, in so far as it is established in the verification of the reasons of substantial public interest referred to in Article 8(4) of Directive 95/46 that, in the light of all the circumstances of the case, the data subject’s fundamental rights guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union override the rights of potentially interested internet users protected by Article 11 of the Charter.

ID: 464e0c8c-a5fb-4751-9258-068299b74b22

Judgment of 7 May 2009, C-553/07 (  
Rijkeboer  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to rectification   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to restriction of processing   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Notification obligation to recipients   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to object   
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Right to an effective judicial remedy against a controller or processor   
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Right to compensation and liability   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Information to be provided in case of direct collection   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
 Information to be provided in case of indirect collection   
   
JUDGMENT OF THE COURT (Third Chamber)  
7 May 2009 (\*)  
(Protection of individuals with regard to the processing of personal data – Directive 95/46/EC – Respect for private life – Erasure of data – Right of access to data and to information on the recipients of data – Time-limit on the exercise of the right to access)  
In Case C-553/07,  
REFERENCE for a preliminary ruling under Article 234 EC made by the Raad van State (Netherlands), by decision of 5 December 2007, received at the Court on 12 December 2007, in the proceedings  
College van burgemeester en wethouders van Rotterdam  
v  
M.E.E. Rijkeboer,  
THE COURT (Third Chamber),  
composed of A. Rosas, President of the Chamber, A. Ó Caoimh, J. Klučka, U. Lõhmus and P. Lindh (Rapporteur), Judges,  
Advocate General: D. Ruiz-Jarabo Colomer,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 20 November 2008,  
after considering the observations submitted on behalf of:  
–        the College van burgemeester en wethouders van Rotterdam, by R. de Bree, advocaat,  
–        M.E.E. Rijkeboer, by W. van Bentem, juridisch adviseur,  
–        the Netherlands Government, by C.M. Wissels and C. ten Dam, acting as Agents,  
–        the Czech Government, by M. Smolek, acting as Agent,  
–        the Greek Government, by E.-M. Mamouna and V. Karra, acting as Agents,  
–        the Spanish Government, by M. Muñoz Pérez, acting as Agent,  
–        the Government of the United Kingdom of Great Britain and Northern Ireland, by Z. Bryanston-Cross and H. Walker, acting as Agents, and by J. Stratford, Barrister,  
–        the Commission of the European Communities, by R. Troosters and C. Docksey, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 22 December 2008,  
gives the following  
Judgment  
1        The reference for a preliminary ruling relates to the interpretation of Article 12(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31; ‘the Directive’).  
2        This reference has been made in the context of proceedings between Mr Rijkeboer and the College van burgemeester en wethouders van Rotterdam (Board of Aldermen of Rotterdam; ‘the College’) regarding the partial refusal of the College to grant Mr Rijkeboer access to information on the disclosure of his personal data to third parties during the two years preceding his request for that information.   
   
Legal context  
   
Community legislation  
3        Recitals 2 and 10 in the preamble to the Directive, relating to fundamental rights and freedoms, state:  
‘(2)      Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;  
…  
(10)      Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law ...’  
4        Pursuant to recital 25 in the preamble to the Directive, the principles of protection must be reflected, on the one hand, in the obligations imposed on persons responsible for processing, in particular regarding data quality, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.   
5        Recital 40 in the preamble to the Directive, which relates to the obligation to inform a data subject when the data have not been gathered from him, states that there will be no such obligation if the provision of information to the data subject proves impossible or would involve disproportionate efforts and that, in that regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.  
6        Pursuant to recital 41 in the preamble to the Directive, any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing.  
7        Article 1, entitled ‘Object of the Directive’, reads as follows:  
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
8        The concept of ‘personal data’ is defined in Article 2(a) of the Directive as any information relating to an identified or identifiable natural person (‘data subject’).   
9        The Directive defines, in Article 2(b) thereof, ‘processing of personal data’ as:  
‘any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction’.  
10      In accordance with Article 2(d) of the Directive, the ‘controller’ is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.  
11      Article 2(g) of the Directive defines ‘recipient’ as a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not, as defined in Article 2(f) of the Directive.  
12      Article 6 of the Directive sets out the principles relating to data quality. With regard to storage, Article 6(1)(e) provides that Member States are to ensure that personal data are ‘kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use’.  
13      Articles 10 and 11 of the Directive set out the information with which the controller or his representative must provide a data subject, either where data relating to him are collected from him or where such data have not been collected from him.  
14      Article 12 of the Directive, entitled ‘Right of access’, states as follows:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
(a)      without constraint, at reasonable intervals and without excessive delay or expense:  
–        confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,  
–        communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,  
–        knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
(c)      notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.’  
15      Article 13(1) of the Directive, entitled ‘Exemptions and restrictions’, authorises Member States to derogate, inter alia, from Articles 6 to 12 thereof, if necessary to safeguard certain public interests, including national security, defence, the prevention, investigation, detection and prosecution of criminal offences and other interests, namely, the protection of the data subject or of the rights and freedoms of others.   
16      Article 14 of the Directive provides that Member States are to grant the data subject the right, on certain grounds, to object to the processing of data relating to him.   
17      In accordance with the second subparagraph of Article 17(1) of the Directive, Member States are to provide that the controller must implement appropriate technical and organisational measures which, having regard to the state of the art and the cost of their implementation, are to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.   
18      Pursuant to Articles 22 and 23(1) of the Directive, Member States are to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question and to provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.   
   
National legislation  
19      The Directive was transposed into Netherlands law by a general provision, the Law on the protection of personal data (Wet bescherming persoonsgegevens). Furthermore, certain laws were adapted in order to take account of the Directive. Such is the case of the Law at issue in the main proceedings, that is to say, the Law on personal data held by local authorities (Wet gemeentelijke basisadministratie persoonsgegevens, Stb. 1994, No 494; ‘the Wet GBA’).  
20      Article 103(1) of the Wet GBA provides that, on request, the College must notify a data subject in writing, within four weeks, whether data relating to him from the local authority personal records have, in the year preceding the request, been disclosed to a purchaser or to a third party.  
21      In accordance with Article 110 of the Wet GBA, the College is to retain details of any communication of data for one year following that communication, unless that communication is apparent in another form in the database.  
22      It is apparent from the written observations of the College that the data held by the local authority include, in particular, the name, the date of birth, the personal identity number, the social security/tax number, the local authority of registration, the address and date of registration at the local authority, civil status, guardianship, the custody of minors, the nationality and residence permit of aliens.   
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
23      By letter of 26 October 2005, Mr Rijkeboer requested the College to notify him of all instances in which data relating to him from the local authority personal records had, in the two years preceding the request, been disclosed to third parties. He wished to know the identity of those persons and the content of the data disclosed to them. Mr Rijkeboer, who had moved to another municipality, wished to know in particular to whom his former address had been disclosed.   
24      By decisions of 27 October and 29 November 2005, the College complied with that request only in part by notifying him only of the data relating to the period of one year preceding his request, by application of Article 103(1) of the Wet GBA.  
25      Communication of the data is registered and stored in electronic form in accordance with the ‘Logisch Ontwerp GBA’ (GBA Logistical Project). This is an automated system established by the Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (Netherlands Ministry of the Interior and Home Affairs). It is apparent from the reference for a preliminary ruling that the data requested by Mr Rijkeboer dating from more than one year prior to his request were automatically erased, which accords with the provisions of Article 110 of the Wet GBA.  
26      Mr Rijkeboer lodged a complaint with the College against the refusal to give him the information relating to the recipients to whom data regarding him had been disclosed during the period before the year preceding his request. That complaint having been rejected by decision of 13 February 2006, Mr Rijkeboer brought an action before the Rechtbank Rotterdam.   
27      That court upheld the action, taking the view that the restriction on the right to information on provision of data to the year before the request, as provided for in Article 103(1) of the Wet GBA, is at variance with Article 12 of the Directive. It also held that the exceptions referred to in Article 13 of that directive are not applicable.  
28      The College appealed against that decision to the Raad van State. That court finds that Article 12 of the Directive on rights of access to data does not indicate any time period within which it must be possible for those rights to be exercised. In its view, that article does not necessarily, however, preclude Member States from imposing a time restriction in their national legislation on the data subject’s right to information concerning the recipients to whom personal data have been provided, but the court has doubts in that regard.  
29      In those circumstances the Raad van State decided to stay the proceedings and to refer the following question to the Court for a preliminary ruling:  
‘Is the restriction, provided for in the [Netherlands] Law [on local authority personal records], on the communication of data to one year prior to the relevant request compatible with Article 12(a) of [the] Directive …, whether or not read in conjunction with Article 6(1)(e) of that directive and the principle of proportionality?’   
   
The question referred  
30      It should be recalled at the outset that, under the system of judicial cooperation established by Article 234 EC, it is for the Court of Justice to interpret provisions of Community law. As far as concerns national provisions, under that system their interpretation is a matter for the national courts (see Case C-449/06   
Gysen  
 [2008] ECR I-553, paragraph 17).  
31      Accordingly, the question referred by the national court should be understood, essentially, as seeking to determine whether, pursuant to the Directive and, in particular, to Article 12(a) thereof, an individual’s right of access to information on the recipients or categories of recipient of personal data regarding him and on the content of the data communicated may be limited to a period of one year preceding his request for access.   
32      That court highlights two provisions of the Directive, that is to say, Article 6(1)(e) on the storage of personal data and Article 12(a) on the right of access to those data. However, neither that court nor any of the parties which submitted observations to the Court has raised the question of the exceptions set out in Article 13 of the Directive.  
33      Article 6 of the Directive deals with the quality of the data. Article 6(1)(e) requires Member States to ensure that personal data are kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The data must therefore be erased when those purposes have been served.  
34      Article 12(a) of the Directive provides that Member States are to guarantee data subjects a right of access to their personal data and to information on the recipients or categories of recipient of those data, without setting a time-limit.  
35      Those two articles seek, therefore, to protect the data subject. The national court wishes to know whether there is a link between those two articles in that the right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed could depend on the length of time for which those data are stored.  
36      The observations submitted to the Court give different points of view on the interaction between those two provisions.  
37      The College and the Netherlands, Czech, Spanish and United Kingdom Governments submit that the right of access to information on the recipients or categories of recipients referred to in Article 12(a) of the Directive exists only in the present and not in the past. Once the data have been erased in accordance with national legislation, the data subject can no longer have access to them. That consequence does not run contrary to the Directive.   
38      The College and the Netherlands Government also submit that Article 103(1) of the Wet GBA, pursuant to which the local authority is to inform a data subject, on request, of data relating to him which, in the year preceding the request, have been disclosed to recipients, goes beyond the requirements laid down in the Directive.  
39      The Commission and the Greek Government submit that the Directive provides for a right of access not only in the present but also for the period preceding the request for access. However, their views diverge with regard to the exact duration of that right of access.  
40      In order to assess the scope of the right of access which the Directive must make possible, it is appropriate, first, to determine what data are covered by the right of access and, next, to turn to the objective of Article 12(a) examined in the light of the purposes of the Directive.  
41      A case such as that of Mr Rijkeboer involves two categories of data.  
42      The first concerns personal data kept by the local authority on a person, such as his name and address, which constitute, in the present case, the basic data. It is apparent from the oral observations submitted by the College and the Netherlands Government that those data may be stored for a long time. They constitute ‘personal data’ within the meaning of Article 2(a) of the Directive, because they represent information relating to an identified or identifiable natural person (see, to that effect, Joined Cases C-465/00, C-138/01 and C-139/01   
Österreichischer Rundfunk and Others  
 [2003] ECR I-4989, paragraph 64; Case C-101/01   
Lindqvist  
 [2003] ECR I-12971, paragraph 24; and Case C-524/06   
Huber  
 [2008] ECR I-0000, paragraph 43).   
43      The second category concerns information on recipients or categories of recipient to whom those basic data are disclosed and on the content thereof and thus relates to the processing of the basic data. In accordance with the national legislation at issue in the main proceedings, that information is stored for only one year.  
44      The time-limit on the right of access to information on the recipient or recipients of personal data and on the content of the data disclosed, which is referred to in the main proceedings, thus concerns that second category of data.  
45      In order to determine whether or not Article 12(a) of the Directive authorises such a time-limit, it is appropriate to interpret that article having regard to its objective examined in the light of the purposes of the Directive.  
46      Pursuant to Article 1 of the Directive, its purpose is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and thus to permit the free flow of personal data between Member States.   
47      The importance of protecting privacy is highlighted in recitals 2 and 10 in the preamble to the Directive and emphasised in the case-law of the Court (see, to that effect,   
Österreichischer Rundfunk and Others  
, paragraph 70;   
Lindqvist  
, paragraphs 97 and 99; Case C-275/06   
Promusicae  
 [2008] ECR I-271, paragraph 63; and Case C-73/07   
Satakunnan Markkinapörssi and Satamedia  
 [2008] ECR I-0000, paragraph 52).  
48      Furthermore, as follows from recital 25 in the preamble to the Directive, the principles of protection must be reflected, on the one hand, in the obligations imposed on persons responsible for processing, in particular regarding data quality – the subject-matter of Article 6 of the Directive – and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request rectification and even to object to processing in certain circumstances.  
49      That right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients. As is stated in recital 41 in the preamble to the Directive, in order to carry out the necessary checks, the data subject must have a right of access to the data relating to him which are being processed.   
50      In that regard, Article 12(a) of the Directive provides for a right of access to basic data and to information on the recipients or categories of recipient to whom the data are disclosed.  
51      That right of access is necessary to enable the data subject to exercise the rights set out in Article 12(b) and (c) of the Directive, that is to say, where the processing of his data does not comply with the provisions of the Directive, the right to have the controller rectify, erase or block his data, (paragraph (b)), or notify third parties to whom the data have been disclosed of that rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort (paragraph (c)).  
52      That right of access is also necessary to enable the data subject to exercise his right referred to in Article 14 of the Directive to object to his personal data being processed or his right of action where he suffers damage, laid down in Articles 22 and 23 thereof.   
53      With regard to the right to access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed, the Directive does not make it clear whether that right concerns the past and, if so, what period in the past.  
54      In that regard, to ensure the practical effect of the provisions referred to in paragraphs 51 and 52 of the present judgment, that right must of necessity relate to the past. If that were not the case, the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered.  
55      A question arises as to the scope of that right in the past.  
56      The Court has already held that the provisions of the Directive are necessarily relatively general since it has to be applied to a large number of very different situations and that the Directive includes rules with a degree of flexibility, in many instances leaving to the Member States the task of deciding the details or choosing between options (see   
Lindqvist  
, paragraph 83). Thus, the Court has recognised that, in many respects, the Member States have some freedom of action in implementing the Directive (see   
Lindqvist  
, paragraph 84). That freedom, which becomes apparent with regard to the transposition of Article 12(a) of the Directive, is not, however, unlimited.  
57      The setting of a time-limit with regard to the right to access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed must allow the data subject to exercise the different rights laid down in the Directive and referred to in paragraphs 51 and 52 of the present judgment.  
58      The length of time the basic data are to be stored may constitute a useful parameter without, however, being decisive.  
59      The scope of the Directive is very wide, as the Court has already held (see   
Österreichischer Rundfunk and Others  
, paragraph 43, and   
Lindqvist  
, paragraph 88), and the personal data covered by the Directive are varied. The length of time such data are to be stored, defined in Article 6(1)(e) of the Directive according to the purposes for which the data were collected or for which they are further processed, can therefore differ. Where the length of time for which basic data are to be stored is very long, the data subject’s interest in exercising the rights to object and to remedies referred to in paragraph 57 of the present judgment may diminish in certain cases. If, for example, the relevant recipients are numerous or there is a high frequency of disclosure to a more restricted number of recipients, the obligation to keep the information on the recipients or categories of recipient of personal data and on the content of the data disclosed for such a long period could represent an excessive burden on the controller.  
60      The Directive does not require Member States to impose such burdens on the controller.  
61      Accordingly, Article 12(c) of the Directive expressly provides for an exception to the obligation on the controller to notify third parties to whom the data have been disclosed of any correction, erasure or blocking, namely, where this proves impossible or involves a disproportionate effort.   
62      In accordance with other sections of the Directive, account may be taken of the disproportionate nature of other possible measures. With regard to the obligation to inform the data subject, recital 40 in the preamble to the Directive states that the number of data subjects and the age of the data may be taken into consideration. Furthermore, in accordance with Article 17 of the Directive concerning security of processing, Member States are to provide that the controller must implement appropriate technical and organisational measures which, having regard to the state of the art and the cost of their implementation, are to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.  
63      Analogous considerations are relevant with regard to the fixing of a time-limit on the right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed. In addition to the considerations referred to in paragraph 57 of the present judgment, a number of parameters may accordingly be taken into account by the Member States, in particular applicable provisions of national law on time-limits for bringing an action, the more or less sensitive nature of the basic data, the length of time for which those data are to be stored and the number of recipients.  
64      Thus it is for the Member States to fix a time-limit for storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to rectification, erasure and blocking of the data in the event that the processing of the data does not comply with the Directive, and rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.  
65      Moreover, when fixing that time-limit, it is appropriate to take account also of the obligations which following from Article 6(e) of the Directive to ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.  
66      In the present case, rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the verifications necessary in the light of the considerations set out in the preceding paragraphs.  
67      Having regard to the foregoing considerations, the argument of some Member States that application of Articles 10 and 11 of the Directive renders superfluous a grant in respect of the past of a right to access to information on the recipients or categories of recipient referred to in Article 12(a) of the Directive cannot be accepted.  
68      Articles 10 and 11 impose obligations on the controller or his representative to inform the data subject, in certain circumstances, in particular of the recipients or categories of recipient of the data. The controller or his representative must communicate that information to the data subject of their own accord, inter alia when the data are collected or, if the data are not collected directly from the data subject, when the data are registered or, possibly, when the data are disclosed to a third party.  
69      In that way, those provisions are intended to impose obligations distinct from those which follow from Article 12(a) of the Directive. Consequently, they in no way reduce the obligation placed on Member States to ensure that the controller is required to give a data subject access to the information on the recipients or categories of recipient and on the data disclosed when that data subject decides to exercise his right to access conferred on him by Article 12(a). Member States must adopt measures transposing, firstly, the provisions of Articles 10 and 11 of the Directive on the obligation to provide information and, secondly, those of Article 12(a) of the Directive, without it being possible for the former to attenuate the obligations following from the latter.  
70      The answer to the question referred must therefore be that:  
–        Article 12(a) of the Directive requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.  
–        Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary.  
   
Costs  
71      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Article 12(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.  
Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary.

ID: 46b435be-3f7a-4bfe-abba-557cca992753

Judgment of 25 Nov 2021, C-102/20 (  
StWL Städtische Werke Lauf  
)  
E-privacy Directive   
 >   
Direct marketing   
   
JUDGMENT OF THE COURT (Third Chamber)  
25 November 2021 (\*)  
(Reference for a preliminary ruling – Directive 2002/58/EC – Processing of personal data and the protection of privacy in the electronic communications sector – Article 2(h) – Concept of ‘electronic mail’ – Article 13(1) – Concept of ‘use of … electronic mail for the purposes of direct marketing’ – Directive 2005/29/EC – Unfair commercial practices – Annex I, point 26 – Concept of ‘persistent and unwanted solicitations by email’ – Advertising messages – Inbox advertising)  
In Case C-102/20,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 30 January 2020, received at the Court on 26 February 2020, in the proceedings  
StWL Städtische Werke Lauf a.d. Pegnitz GmbH  
v  
eprimo GmbH,  
intervening party:  
Interactive Media CCSP GmbH,  
THE COURT (Third Chamber),  
composed of A. Prechal, President of the Second Chamber, acting as President of the Third Chamber, J. Passer, F. Biltgen, L.S. Rossi (Rapporteur) and N. Wahl, Judges,  
Advocate General: J. Richard de la Tour,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        eprimo GmbH, by R. Hall, Rechtsanwalt,  
–        Interactive Media CCSP GmbH, by D. Frey and M. Rudolph, Rechtsanwälte,  
–        the Portuguese Government, by L. Inez Fernandes, A. Guerra and P. Barros da Costa, acting as Agents,  
–        the European Commission, by C. Hödlmayr, F. Wilman, N. Ruiz García and S. Kalėda, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 24 June 2021,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2(h) and Article 13(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), and Annex I, point 26, to Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ 2005 L 149, p. 22).  
2        The request has been made in two sets of proceedings between StWL Städtische Werke Lauf a.d. Pegnitz GmbH (‘StWL’) and eprimo GmbH, which are two companies that supply electricity to final customers, concerning an advertising activity by Interactive Media CCSP GmbH, at eprimo’s request, consisting in posting advertising messages in the inboxes of users of the free email service ‘T-Online’.  
   
Legal context  
   
EU law  
3        Recitals 4 and 40 of Directive 2002/58 read as follows:  
‘(4)      Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [(OJ 1998 L 24, p. 1)] translated the principles set out in Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)] into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.  
…  
(40)      Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and emails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, [European Union-wide] rules for businesses and users.’  
4        Article 1(1) of that directive provides:  
‘This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the [European Union].’  
5        Under Article 2(d), (f) and (h), of the directive, entitled ‘Definitions’:  
‘The following definitions shall also apply:  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
…  
(f)      “consent” by a user or subscriber corresponds to the data subject’s consent in Directive 95/46/EC  
…  
(h)      “electronic mail” means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient.’  
6        Article 13(1) of the same directive, entitled ‘Unsolicited communications’, provides:  
‘The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.’  
7        Recital 67 of Directive 2009/136 reads:  
‘Safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, [multi-media messages (MMS)] and other kinds of similar applications.’  
8        Article 2(h) of Directive 95/46/EC provides:  
‘For the purposes of this Directive:  
…  
(h)      “the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.’  
9        Article 94(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2), entitled ‘Repeal of Directive 95/46/EC’ provides:  
‘References to the repealed Directive shall be construed as references to this Regulation. …’  
10      Article 4(11) of that regulation is worded as follows:  
‘For the purposes of this Regulation:  
…  
(11)      “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.  
11      Recital 17 of Directive 2005/29 is worded as follows:  
‘(17)      It is desirable that those commercial practices which are in all circumstances unfair be identified to provide greater legal certainty. Annex I therefore contains the full list of all such practices. These are the only commercial practices which can be deemed to be unfair without a case-by-case assessment against the provisions of Articles 5 to 9. The list may only be modified by revision of the Directive.’  
12      Article 5 of the directive provides:  
‘1.      Unfair commercial practices shall be prohibited.  
2.      A commercial practice shall be unfair if:  
(a)      it is contrary to the requirements of professional diligence,  
and  
(b)      it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.  
…  
4. In particular, commercial practices shall be unfair which:  
(a)      are misleading as set out in Articles 6 and 7,  
or  
(b)      are aggressive as set out in Articles 8 and 9.  
5.      Annex I contains the list of those commercial practices which shall in all circumstances be regarded as unfair. The same single list shall apply in all Member States and may only be modified by revision of this Directive.’  
13      Article 8 of that directive states:  
‘A commercial practice shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer’s freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise.’  
14      Point 26 of Annex I to that directive, which contains the list of commercial practices considered unfair in all circumstances, provides:  
‘Aggressive commercial practices  
…  
(26)      Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation. This is without prejudice to … Directives 95/46/EC and [2002/58].’  
   
German law  
15      Paragraph 3(1) and (2) of the Gesetz gegen den unlauteren Wettbewerb (Law against unfair competition, of 3 July 2004, BGBl. 2004 I, p. 1414, ‘the UWG’) in the version applicable in the dispute in the main proceedings, provides:  
‘(1)      Unfair commercial practices shall be unlawful.  
(2)      Commercial practices addressed to or reaching consumers are unfair where they do not meet the level of diligence required of undertakings and are likely to materially distort the economic behaviour of consumers.’  
16      Under Paragraph 5a(6) of the UWG, entitled ‘Misleading by ommission’:  
‘Unfairness also occurs … where the commercial intent of a commercial practice is not identified, unless this is directly apparent from the context, and where such failure to identify the commercial intent is likely to cause the consumer to take a transactional decision which he or she would not have taken otherwise.’  
17      Paragraph 7 of the UWG provides:  
‘(1)      Commercial practices which cause unacceptable nuisance to a market participant shall be unlawful. That applies in particular to advertising that takes place although it is clear that the market participant concerned does not want it.  
(2)      Unacceptable nuisance must always be assumed in the case of:  
1.      advertising using a means of commercial communication for distance marketing not listed in points 2 and 3, whereby a consumer is persistently solicited although he or she clearly does not want this;  
…  
3.      advertising using an automated calling machine, a fax machine or electronic mail, without the express prior consent of the recipient, or  
4.      advertising in the form of a message  
(a)      where the identity of the sender on whose behalf the communication is made is disguised or concealed …  
…’  
18      Paragraph 8 of the UWG provides:  
‘(1)      Where a person engages in an unlawful commercial practice under Paragraphs 3 or 7, an action to eliminate that unlawful practice may be brought against that person and, where there is a risk of recurrence, an action to obtain a prohibitory injunction. The right to seek a prohibitory injunction exists where such a practice in breach of Paragraph 3 or Paragraph 7 threatens to occur.  
…  
(3)      The rights under subparagraph 1 shall be conferred on:  
1.      any competitor;  
…’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
19      It is apparent from the order for reference that StWL and eprimo are two competing electricity suppliers. At the request of eprimo, Interactive Media CCSP, an advertising agency, inserted advertisements into the email inboxes of users of the T-Online free email service. That service is funded by advertising paid for by advertisers and provided free to users.  
20      Those advertisements appeared in the private email inboxes of those users, specifically in the section in which incoming emails are listed, and were inserted between the emails received.  
21      Those users thus received, on 12 December 2016, 13 January 2017 and 15 January 2017, advertising messages in their inboxes. Entries appeared therein which were not visually distinguishable in the list from other emails in the user’s account except for the fact that: (i) the date was replaced by the word ‘  
Anzeige  
’ (advertisement),  
(ii) no sender was mentioned and (iii) the text appeared against a grey background. The ‘subject’ section corresponding to that entry in the list contained text intended to promote advantageous prices for electricity and gas services.  
22      From a technical point of view, a JavaScript code of an advertising server (TAG) is connected with the place in question in the inbox on the internet page consulted by the user of such an email inbox. For that reason, when a user opens the internet page, a request   
(Adrequest)  
 is sent to the advertising server in order to randomly select an advertising banner from a basket constituted by advertisers and transmit it, such that it appears in the user’s inbox. If the user clicks on the advertisement displayed, the input is conveyed to the advertising server, which records it and redirects the browser to the advertiser’s website.  
23      The functionality of the T-Online email service treats the insertion of the advertising messages in question into users’ inboxes differently from ordinary emails: the advertising message, which appears in the form of an email, may be deleted from the list, but may not be archived, altered or forwarded, and it is not possible to reply to it. Finally, the advertising message is not counted amongst the total number of emails in the inbox, and nor does it take up storage space.  
24      StWL considered that that advertising practice involving the use of email without the recipient’s express prior consent was contrary to the rules of unfair competition in that it constituted an ‘unacceptable nuisance’ within the meaning of Paragraph 7(2)(3) of the UWG and that it was misleading, within the meaning of Paragraph 5a(6) of the UWG. On that basis, StWL commenced an action to desist against eprimo before the Landgericht Nürnberg-Fürth (Regional Court, Nuremberg-Fürth, Germany). That court upheld StWL’s application and ordered eprimo, on pain of a fine, to cease disseminating, to final consumers, such advertising relating to the supply of electricity via the T-online.de email account.  
25      On an appeal brought by eprimo before the Oberlandesgericht Nürnberg (Higher Regional Court, Nuremberg, Germany), that court considered that the contested placement of advertising in the T-Online private email inbox did not constitute an unlawful commercial practice under competition law.  
26      In particular, according to that court, first, the defendant’s advertising was not an unacceptable nuisance involving the use of ‘electronic mail’, within the meaning of Paragraph 7(2)(3) of the UWG since that advertising could not be regarded as an ‘electronic mail’, within the meaning of that provision. In any event, the advertising at issue did not entail, for the user of the T-Online email service, any charges or costs greater than the ‘normal’ nuisance occasioned by any advertising and did not therefore cause an ‘unacceptable nuisance’ within the meaning of the general provision contained in the first sentence of Paragraph 7(1) of the UWG, in particular having regard to the fact that the email service was provided free of charge.  
27      Secondly, that court found that the advertising at issue was not unlawful under Paragraph 7(2)(4)(a) of the UWG, since it was not advertising in the form of messages. Paragraph 7(2)(1) of the UWG was also inapplicable, since it presupposes ‘solicitation’, in the sense of ‘conduct inconveniencing’ a consumer, which was lacking in the present case. Furthermore, the defendant’s advertisements, which did not conceal the fact that they were advertisements, could not be considered to be unfair on the ground that they were misleading, within the meaning of Paragraph 5a(6) of the UWG.  
28      Hearing an appeal on a point of law brought before it by StWL, the Bundesgerichtshof (Federal Court of Justice, Germany) considers that the success of the appeal depends on the interpretation of Article 2(d) and (h) and Article 13(1) of Directive 2002/58 and of Annex I, point 26, to Directive 2005/29.  
29      According to the referring court, the conduct for which eprimo is criticised may be unlawful under Paragraph 7(2)(3) of the UWG, which transposes Article 13(1) of Directive 2002/58. It states that it is also possible that the advertising is unlawful under Paragraph 7(2)(1) of the UWG, which transposes point 26 of Annex I to Directive 2005/29.  
30      In that regard, the referring court seeks clarification from the Court of Justice regarding the criteria governing the concept of ‘electronic mail’, within the meaning of Article 2(h) of Directive 2002/58 and the concept of ‘use’ of the latter for the purposes of direct marketing within the meaning of Article 13(1) thereof. In addition, the referring court asks the Court to specify the criteria for ‘solicitation’, within the meaning of point 26 of Annex I to Directive 2005/29.  
31      In those circumstances, the Bundesgerichtshof (Federal Court of Justice) decided to stay the proceedings and refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Does the concept of “sending” within the meaning of Article 2(h) of Directive [2002/58] cover a situation in which a message is not transmitted by a user of an electronic communications service, via a service provider, to the electronic “address” of a second user, but, as a consequence of the opening of the password-protected internet page of an email account, is automatically displayed by ad servers in certain areas designated for that purpose in the email inbox of a randomly selected user (inbox advertising)?  
(2)      Does the collection of a message within the meaning of Article 2(h) of Directive [2002/58] presuppose that, after becoming aware of the existence of a message, the recipient triggers the programmatically prescribed transmission of the message data by making an intentional collection request, or is it sufficient for the appearance of a message in an email account inbox to be triggered by the user opening the password-protected internet page of his or her e-mail account?  
(3)      Does a message, which is not sent to an individual recipient already specifically identified prior to transmission but is inserted into the inbox of a randomly selected user, constitute an electronic mail within the meaning of Article 13(1) of Directive [2002/58]?  
(4)      Is electronic mail used for the purposes of direct marketing, within the meaning of Article 13(1) of Directive [2002/58], only where the user is found to be the subject of a burden that is greater than a nuisance?  
(5)      Does individual advertising meet the conditions governing the presence of “solicitation”, for the purposes of the first sentence of point 26 of Annex I to Directive [2005/29], only where a customer is contacted via a medium traditionally used for individual communication between a sender and a recipient, or is it sufficient if – as with the advertisement at issue in the present case – an individual connection is established by the fact that the advertisement is displayed in the inbox of a private email account, and thus in a section in which the customer expects to find messages addressed to him or her personally?’  
   
Consideration of the questions referred  
   
The first to fourth questions  
32      By its first to fourth questions, which it is appropriate to examine together, the referring court asks, in essence, first, whether Article 2(h) and Article 13(1) of Directive 2002/58 must be interpreted as meaning that the criteria governing the concept of ‘electronic mail’, within the meaning of those provisions, are met when an advertising message displayed following the opening of the internet page, which is protected by a password, corresponding to an email account, in certain spaces allocated for that purpose in the electronic inbox of a user selected at random; and, second, whether Article 13(1) of that directive must be interpreted as meaning that such an advertising activity falls within the concept of ‘use of … electronic mail for the purposes of direct marketing’, within the meaning of that provision, which requires that the user of the email service concerned has given his or her prior consent to such activity, only if the user is found to be the subject of a burden that is greater than a nuisance.  
33      In order to reply to those questions, it should be borne in mind that, under Article 1(1) thereof, Directive 2002/58 provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector.  
34      As recital 40 thereof states, that directive intends safeguards to be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and emails, including SMS messages.  
35      Article 2(d) of Directive 2002/58 lays down a broad definition of the concept of ‘communication’ that includes any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service.  
36      In that regard, Article 13(1) of that directive, entitled ‘Unsolicited communications’ allows the use of various types of communication, namely automated calling machines without human intervention (automatic calling machines), facsimile machines, and emails, for the purposes of direct marketing, on the condition that they target subscribers or users who have given their prior consent.  
37      In order to apply that provision, it is necessary therefore to ascertain, in the first place, whether the type of communication used for those direct marketing purposes is amongst those covered by that provision; in the second place, whether such a communication has the purpose of direct marketing; and, in the third place, whether the requirement to obtain prior consent from the user has been complied with.  
38      As regards, in the first place, the means of electronic communication through which direct marketing is conducted, it should be noted, at the outset, as the Advocate General observed in point 53 of his Opinion, that the list of means of communication referred to in recital 40 and in Article 13(1) of that directive is not exhaustive.  
39      First, Directive 2009/136, which amended Directive 2002/58, refers, in recital 67 thereof, to kinds of communication other than those mentioned in Directive 2002/58 when it states that the safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail ‘should also be applicable to SMS, MMS and other kinds of similar applications’.   
Second, as specified in recital 4 of Directive 2002/58, the objective of providing an equal level of protection of personal data and privacy for users of publicly available electronic communications services must be ensured ‘regardless of the technologies used’, which confirms that it is necessary to adopt an interpretation that is broad, and evolving from a technological perspective, of the types of communication covered by that directive.  
40      Having made those observations, it must be held that, in the present case, the advertising message at issue in the main proceedings was distributed to the persons concerned using a means of communication expressly referred to in Article 13(1) of Directive 2002/58, namely electronic mail.  
41      In that regard, from the recipient’s point of view, the advertising message is displayed in the user’s email inbox, namely in a space normally reserved for private emails. The user is only able to free that space in order to obtain a view of all of his or her exclusively private emails after having checked the content of that advertising message, and only after having actively deleted it. If the user clicks on an advertising message, such as the one at issue in the main proceedings, he or she is redirected to an internet site containing the advertising in question, rather than continuing with the reading of his or her private emails.  
42      Thus, by contrast with advertising banners or pop-up windows, which are displayed at the edges of, or separately from, the list of private messages, the appearance of the advertising messages at issue in the main proceedings within the list of the user’s private emails, impedes access to those emails in a manner similar to that used for unsolicited emails (also known as ‘spam’) to the extent that such a method requires the same decision to be taken by the subscriber concerning the processing of those messages.  
43      Moreover, as the Advocate General observed in point 55 of his Opinion, since the advertising messages occupy lines in the inbox that are normally designated for private emails and because of their similarity to the latter, there is a likelihood of confusion between those two categories of messages that may cause a user who clicks on the line corresponding to the advertising message to be redirected unintentionally to a website offering the advertisement at issue instead of continuing to access his or her private emails.  
44      And, as the Commission observed, if advertising entries of any kind are displayed in the inbox of an internet email account, namely in the section in which all of the emails addressed to the user are displayed, that email inbox must be regarded as constituting a means by which the advertising messages concerned are communicated to that user, which involves the use of his or her email for the purposes of direct marketing, within the meaning of Article 13(1) of Directive 2002/58. In other words, the defendant and the intervener in the main proceedings, and also the email service provider involved, use the existence of the list of private emails, taking into account the particular interest and trust of the subscriber with regard to that list, to place their direct advertising, giving it the appearance of a real email.  
45      Proceeding in that manner constitutes a use of electronic mail, within the meaning of Article 13(1) of Directive 2002/58, likely to breach the objective, pursued by that provision, of protecting users from any intrusion into their private life by unsolicited communications for the purposes of direct marketing.  
46      Accordingly, the question of whether advertising messages such as those at issue in the main proceedings themselves fulfil the criteria to be classified as ‘electronic mail’, within the meaning of Article 2(h) of that directive, becomes superfluous in so far as those messages are communicated to the users concerned by means of their email inbox and thus their electronic mail.  
47      As regards, in the second place, the question of whether communications covered by Article 13(1) of that directive are made for the purpose of direct marketing, it must be ascertained whether such a communication pursues a commercial purpose and is addressed directly and individually to a consumer.  
48      In the present case, the very nature of the advertising messages at issue in the main proceedings, which promote services, and the fact that they are distributed in the form of an email such that they are directly displayed in the inbox of the private email service of the user concerned, allows those messages to be classified as communications for the purposes of direct marketing, within the meaning of Article 13(1) of Directive 2002/58.  
49      The fact that the recipient of those advertising messages is chosen at random, which is raised as part of the third question posed by the referring court, cannot call that conclusion into question.  
50      In that regard, it suffices to observe, as the Advocate General has done in point 61 of his Opinion, that the random or predefined selection of the recipient is not one of the conditions for the application of Article 13(1) of Directive 2002/58. In other words, it is irrelevant whether the advertising at issue is addressed to a predetermined and individually identified recipient or is sent on a mass, random basis to multiple recipients. What matters is that there is a communication for a commercial purpose, which reaches, directly and individually, one or more email service users by being inserted in the inboxes of those users’ email accounts.  
51      The recipients of such advertising messages are individual, inter alia, in their capacity as users of a provider’s individual email service in so far as the user obtains access to his or her inbox only after having entered his or her registration data and password. Consequently, the display occurs following that authentication procedure by the user in a private space reserved to him or her and which is intended for the consultation of private content, in the form of emails.  
52      In the third place, as regards specifically the requirement to obtain prior consent, laid down in Article 13(1) of Directive 2002/58, it must be recalled that a communication which falls within the field of application of that provision is allowed, on condition that its recipient has given prior consent.  
53      In that respect, it is clear from Article 2(f) of Directive 2002/58, read in conjunction with Article 94(2) of Regulation 2016/679, that such consent must meet the requirements under Article 2(h) of Directive 95/46 or Article 4(11) of that regulation, depending on which of those two rules is applicable   
ratione temporis  
 to the facts at issue in the main proceedings.  
54      Article 2(h) of Directive 95/46, defines the term ‘consent’ as meaning ‘any freely given specific and informed indication of his [or her] wishes by which the data subject signifies his [or her] agreement to personal data relating to him [or her] being processed’.  
55      That same requirement also applies in the context of Regulation 2016/679. Indeed, Article 4(11) of that regulation defines the ‘consent of the data subject’ as meaning that it requires a ‘freely given, specific, informed and unambiguous’ indication of the data subject’s wishes in the form of a statement or by ‘a clear affirmative action’ signifying agreement to the processing of personal data relating to him or her.  
56      In the case of an action to bring about the end of an illicit commercial practice, such as the case at issue in the main proceedings, it is not inconceivable that, as the Advocate General observed in point 50 of his Opinion, supposing the proceedings brought by StWL seek an order that eprimo refrain from future action, Regulation 2016/679 would be applicable   
ratione temporis  
 to the dispute in the main proceedings although the facts giving rise to that dispute occurred prior to 25 May 2018, the date on which that regulation became applicable, since Directive 95/46 was repealed with effect from that date.  
57      It follows from the foregoing that such consent must be indicated, at least, in a manifestation of a free, specific and informed wish on the part of the person concerned (‘the data subject’).  
58      In the present case, it is clear from the case file submitted to the Court that, during the registration process for the email address at issue in the main proceedings, the T-Online email service is offered to users in the form of two categories of email services, namely, first, a free email service funded by advertising and, second, a paid-for email service, without advertising. Thus, users who choose the free service, as in the case in the main proceedings, accept that they will receive advertisements in order not to pay any consideration in exchange for the use of that email service.  
59      In that regard, it is however for the referring court to determine whether the user concerned, having opted for the free T-Online email service, was duly informed of precise means of distribution of such advertising and in fact consented to receiving advertising messages such as those at issue in the main proceedings. In particular, it is necessary for that court to be satisfied, first, that that user was clearly and precisely informed in particular of the fact that advertising messages are displayed within the list of private emails received and, second, that he or she specifically and on a fully informed basis, indicated his or her consent to receive such advertising messages (see, to that effect, judgment of 11 November 2020,   
Orange Romania  
, C-61/19, EU:C:2020:901, paragraph 52).  
60      Finally, in response to the fourth question by which the referring court asks whether, in order for advertising such as that at issue in the main proceedings to be classified as ‘use of … electronic mail for the purposes of direct marketing’, within the meaning of Article 13(1) of Directive 2002/58, it is necessary to find that the burden to which the user is subject is greater than a nuisance, it must be held that the directive does not require such a test to be met.  
61      As the Advocate General observed in point 62 of his Opinion, it is clear from recital 40 of that directive that the requirement to obtain prior consent laid down in that provision stems, in particular, from the fact that unsolicited communications for direct marketing purposes may ‘impose a burden and/or cost on the recipient’. Since such communications fall within the scope of Article 13(1) of Directive 2002/58, it is not therefore necessary to ascertain whether the resulting burden for the recipient is greater than a nuisance.  
62      In the present case, it is moreover common ground that advertising activity such as that at issue in the main proceedings does indeed impose a burden on the user concerned to the extent that, as has been observed in paragraph 42 of this judgment, the appearance of advertising messages within the list of the user’s private emails in a manner similar to that used for unsolicited emails (spam), requires the same decisions to be taken by the subscriber as regards the processing of those messages.  
63      Having regard to all the foregoing considerations, the answer to the first to fourth questions is that Article 13(1) of Directive 2002/58 must be interpreted as meaning that the display, in the inbox of an electronic mail service user, of advertising messages in a form similar to that of real emails, and placed in the same position as those emails, without the fact that recipients are randomly determined or an assessment of the level of intensity and burden imposed on that user being relevant in that regard, constitutes ‘use of … electronic mail for the purposes of direct marketing’, such use being allowed only on the condition that the user was clearly and specifically informed of the distribution methods of such advertising, including within the list of private emails received, and indicated his or her specific and fully informed consent to receive such messages.  
   
The fifth question  
64      By its fifth question, the referring court asks, in essence, whether Annex I, point 26, to Directive 2005/29 must be interpreted as meaning that an activity consisting of the display in the inbox of an email service user of advertising messages in a form similar to that of real emails, and placed in the same position as those emails, falls within the concept of ‘persistent and unwanted solicitations’ of users of email services, within the meaning of that provision.  
65      Article 5 of that directive prohibits, in paragraph 1 thereof, unfair commercial practices and lays down, in paragraph 2, the criteria for determining whether a commercial practice is unfair.  
66      Article 5(4) of that directive provides, in particular, that commercial practices which are ‘misleading’, within the meaning of Articles 6 and 7 of Directive 2005/29, and those which are ‘aggressive’ within the meaning of Articles 8 and 9 of that directive, are unfair.  
67      In that regard, it should be recalled that Directive 2005/29 carries out a complete harmonisation at EU level of the rules relating to unfair commercial practices of undertakings vis-à-vis consumers and establishes, in Annex I thereto, an exhaustive list of 31 commercial practices which, in accordance with Article 5(5) of that directive, are regarded as unfair ‘in all circumstances’. Consequently, as recital 17 of that directive expressly states, these commercial practices alone can be deemed to be unfair in themselves without a case-by-case assessment pursuant to the provisions of Articles 5 to 9 of that directive (judgment of 2 September 2021,   
Peek & Cloppenburg  
, C-371/20, EU:C:2021:674, paragraph 34 and the case-law cited).  
68      Thus, pursuant to Annex I, point 26, to Directive 2005/29, ‘commercial practices which shall be regarded as unfair in all circumstances’ covers, as an aggressive commercial practice, a professional ‘making persistent and unwanted solicitations by telephone, fax, email or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation’.  
69      As has been observed in paragraphs 48, 50 and 51 of this judgment, an advertising message, such as that at issue in the main proceedings, must be regarded as addressing the user concerned directly and individually to the extent that, since it is distributed in the form of an email, it appears directly within the inbox of the private email of the user concerned, within a private space protected by a password, which is reserved to that user and where he or she expects to receive only messages addressed to him or her individually.  
70      For that reason, as the Advocate General observed in point 71 of his Opinion, the effect of that message is therefore similar to that of individual direct marketing, whether or not the advertiser has singled out that specific recipient during the technical preparation of the message in question and whether or not that message is processed differently from emails in terms of storage space and functionalities connected with the processing of a real electronic mail.  
71      In those circumstances, it must be held that such an advertising message constitutes a ‘solicitation’ of email service users, within the meaning of Annex I, point 26, to Directive 2005/29.  
72      That being so, it is necessary next to ascertain whether such a solicitation is ‘persistent and unwanted’ such that it must be prohibited in all circumstances under that provision.  
73      In that regard, it is necessary to observe, first, that, as recalled in paragraph 21 of this judgment, the users concerned received advertising messages in their private email inboxes on three occasions, namely 12 December 2016, 13 January 2017 and 15 January 2017 respectively. In those circumstances, such a solicitation, taking into account also its frequency within a limited period of time, must be regarded as being ‘persistent’ within the meaning of Annex I, point 26, to Directive 2005/29, as the referring court found.  
74      Second, as regards whether such an advertising activity is ‘unwanted’, within the meaning of the same point 26, it is necessary to ascertain whether the display of an advertising message such as that at issue in the main proceedings meets that condition having regard to whether or not consent was given by that user prior to that display and whether that user expressed any opposition to such an advertising practice. Such opposition is furthermore established in the case in the main proceedings, as the referring court found.  
75      Having regard to all the foregoing considerations, the answer to the fifth question is that Annex I, point 26, to Directive 2005/29 must be interpreted as meaning that an activity consisting of the display in the inbox of an email service user of advertising messages in a form similar to that of real emails, and placed in the same position as those emails, falls within the concept of ‘persistent and unwanted solicitations’ of users of email services, within the meaning of that provision, if the display of those advertising messages is, first, sufficiently frequent and regular to be classified as ‘persistent solicitations’ and, second, may be classified as ‘unwanted solicitations’ in the absence of consent having been given by that user prior to that display.  
   
Costs  
76      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 13(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, must be interpreted as meaning that the display, in the inbox of an electronic mail service user, of advertising messages in a form similar to that of real emails, and placed in the same position as those emails, without the fact that recipients are randomly determined or an assessment of the level of intensity and burden imposed on that user being relevant in that regard, constitutes ‘use of … electronic mail for the purposes of direct marketing’, which is permitted only on the condition that the user was clearly and specifically informed of the distribution methods of such advertising, including within the list of private emails received, and the user indicated specific and fully informed consent to receive such messages.  
2.        
Annex I, point 26, to Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’), must be interpreted as meaning that an activity consisting of the display in the inbox of an email service user of advertising messages in a form similar to that of real emails, and placed in the same position as those emails, falls within the concept of ‘persistent and unwanted solicitations’ of users of email services, within the meaning of that provision, if the display of those advertising messages is, first, sufficiently frequent and regular to be classified as ‘persistent solicitations’ and, second, may be classified as ‘unwanted solicitations’ in the absence of consent having been given by that user prior to that display.

ID: 48c899fa-0d71-4ba4-badf-d8898028bdf4

Judgment of 5 Apr 2022, C-140/20 (  
Commissioner of the Garda Síochána and Others  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Location data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
E-privacy Directive   
 >   
Electronic communications   
 >   
Data retention and access of national authorities   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
E-privacy Directive   
 >   
Electronic communications   
 >   
Data retention and access of national authorities   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Location data   
   
JUDGMENT OF THE COURT (Grand Chamber)  
5 April 2022 (\*)  
(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Confidentiality of the communications – Providers of electronic communications services – General and indiscriminate retention of traffic and location data – Access to retained data – Subsequent court supervision – Directive 2002/58/EC – Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Possibility for a national court to restrict the temporal effect of a declaration of the invalidity of national legislation that is incompatible with EU law – Excluded)  
In Case C-140/20,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Supreme Court (Ireland), made by decision of 25 March 2020, received at the Court on 4 August 2016, in the proceedings  
G.D.  
v  
Commissioner of An Garda Síochána,  
Minister for Communications, Energy and Natural Resources,  
Attorney General,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis and N. Jääskinen, Presidents of Chambers, T. von Danwitz (Rapporteur), M. Safjan, F. Biltgen, P.G. Xuereb, N. Piçarra, L.S. Rossi and A. Kumin, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 13 September 2021,  
after considering the observations submitted on behalf of:  
–        G.D., by J. Dunphy, Solicitor, R. Kennedy, Senior Counsel, and R. Farrell, Senior Counsel, and K. McCormack, Barrister-at-Law,  
–        the Commissioner of An Garda Síochána, the Minister for Communications, Energy and Natural Resources and the Attorney General, by M. Browne, S. Purcell, C. Stone and J. Quaney and by A. Joyce, acting as Agents, and by S. Guerin, Senior Counsel, and P. Gallagher, Senior Counsel, D. Fennelly and L. Dwyer, Barristers-at-Law,  
–        the Belgian Government, by P. Cottin and J.-C. Halleux, acting as Agents, and by J. Vanpraet, advocaat,  
–        the Czech Government, by M. Smolek, O. Serdula and J. Vláčil, acting as Agents,  
–        the Danish Government, initially by J. Nymann-Lindegren, M. Jespersen and M. Wolff, and subsequently by M. Wolff and V. Jørgensen, acting as Agents,  
–        the Estonian Government, by A. Kalbus and M. Kriisa, acting as Agents,  
–        the Spanish Government, by L. Aguilera Ruiz, acting as Agent,  
–        the French Government, by E. de Moustier and A. Daniel and by D. Dubois, T. Stéhelin and J. Illouz, acting as Agents,  
–        the Cypriot Government, by I. Neophytou, acting as Agent,  
–        the Netherlands Government, by C.S. Schillemans, M.K. Bulterman and A. Hanje, acting as Agents,  
–        the Polish Government, by B. Majczyna and J. Sawicka, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes and by P. Barros da Costa and I. Oliveira, acting as Agents,  
–        the Finnish Government, by M. Pere and A. Laine, acting as Agents,  
–        the Swedish Government, by O. Simonsson and J. Lundberg and by H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson and H. Eklinder, acting as Agents,  
–        the European Commission, by S.L. Kalėda, H. Kranenborg, M. Wasmeier and F. Wilman, acting as Agents,  
–        the European Data Protection Supervisor, by D. Nardi, N. Stolič and K. Ujazdowski and by A. Buchta, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 18 November 2021,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between G.D. and the Commissioner of An Garda Síochána (Commissioner of the national police force, Ireland), the Minister for Communications, Energy and Natural Resources (Ireland) and the Attorney General, concerning the validity of the Communications (Retention of Data) Act 2011 (‘the 2011 Act’).  
   
Legal context  
   
European Union law  
3        Recitals 2, 6, 7 and 11 of Directive 2002/58 state:  
‘(2)      This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by [the Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of [the Charter].  
…  
(6)      The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.  
(7)      In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.  
…  
(11)      Like Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.’  
4        Article 1 of Directive 2002/58, headed ‘Scope and aim’, provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the [European Union].  
2.      The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.  
3.      This Directive shall not apply to activities which fall outside the scope of [the TFEU], such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.’  
5        Article 2 of Directive 2002/58, headed ‘Definitions’, provides:  
‘Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.  
The following definitions shall also apply:  
(a)      “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  
(c)      “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
…’  
6        Article 3 of Directive 2002/58, headed ‘Services concerned’, provides:  
‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the [European Union], including public communications networks supporting data collection and identification devices.’  
7        Article 5 of the directive, headed ‘Confidentiality of the communications’, provides:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
…  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
8        Article 6 of Directive 2002/58, entitled ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
…’  
9        Article 9 of that directive, entitled ‘Location data other than traffic data’, provides, in paragraph 1 thereof:  
‘Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …’  
10      Article 15 of Directive 2002/58, entitled ‘Application of certain provisions of Directive [95/46]’, provides, in paragraph 1 thereof:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may,   
inter alia  
, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of [EU] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’  
   
Irish law  
11      As stated in the order for reference, the 2011 Act was adopted in order to transpose into the Irish legal order Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).  
12      Section 1 of the 2011 Act defines ‘data’ as ‘traffic data or location data and the related data necessary to identify the subscriber or user’ and a ‘serious offence’ as one which is punishable by imprisonment for a term of five years or more and also those other offences listed in Schedule 1 to that act.  
13      Section 3(1) of the 2011 Act requires all providers of electronic communications services to retain the data referred to in Schedule 2, Part 1, for a period of two years and the data referred to in Schedule 2, Part 2, for a period of one year.  
14      Schedule 2, Part 1, to the 2011 Act applies, inter alia, to fixed network telephony data and mobile telephony data that permit the identification of the source, the destination, and the date and time of the start and end of a communication, the type of communication involved, the type of location and the geographic location of the communications equipment used. In particular, point 6 of Part 1 of Schedule 2 provides for the retention of data necessary to identify the location of mobile communication equipment, those data being, first, the identity of the cell (‘cell ID’) and, second, data identifying the geographical location of cells by reference to their cell ID during the period for which communication data are retained.  
15      Schedule 2, Part 2, to the 2011 Act covers data relating to internet access, internet email and internet telephony and includes, inter alia, the user identification number (‘user ID’) and telephone number, the Internet Protocol (IP) address and the date, time and duration of a communication. The content of communications does not fall within this type of data.  
16      Under sections 4 and 5 of the 2011 Act, service providers must take specified measures to ensure that data are protected against unauthorised access.  
17      Section 6 of the 2011 Act, which lays down the conditions under which a disclosure request may be made, provides in paragraph 1:  
‘A member of the Garda Síochána not below the rank of chief superintendent may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 where that member is satisfied that the data are required for—  
(a)      the prevention, detection, investigation or prosecution of a serious offence,  
(b)      the safeguarding of the security of the State,  
(c)      the saving of human life.’  
18      Section 7 of the 2011 Act requires service providers to comply with disclosure requests referred to in section 6 thereof.  
19      For the purpose of reviewing the decision of the member of the Garda Síochána referred to in section 6 of the 2011 Act, a complaint procedure is provided for in section 10 thereof and a procedure before the designated judge, within the meaning of section 12 thereof, who is responsible for examining the application of the provisions of that act.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
20      In March 2015, G.D. was sentenced to life imprisonment for the murder of a person who disappeared in August 2012 and whose remains were not discovered until September 2013. In the appeal against his conviction, G.D. criticised the first-instance court in particular for having incorrectly admitted as evidence traffic and location data relating to telephone calls, on the ground that the 2011 Act, which governed the retention of that data and on the basis of which the police carrying out the investigation had obtained access to those data, infringed rights conferred on him by EU law. That appeal is currently pending.  
21      In order to be able to contest, as part of the criminal proceedings, the admissibility of that evidence, G.D. brought civil proceedings before the High Court (Ireland) seeking a declaration that some of the provisions of the 2011 Act are invalid. By decision of 6 December 2018, that court upheld G.D.’s submission and held that section 6(1)(a) of that act was incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter. Ireland appealed against that decision to the Supreme Court (Ireland), which is the referring court.  
22      The criminal proceedings pending before the Court of Appeal (Ireland) were stayed until the delivery of the referring court’s decision in the main civil proceedings.  
23      Before the referring court, Ireland submitted that, in order to determine whether interference with the right to private life enshrined in Article 7 of the Charter as a result of the retention of traffic and location data under the 2011 Act is proportionate, it is necessary to examine the objectives of the regime established by that law as a whole. In addition, according to that Member State, that act established a detailed framework governing access to retained data by virtue of which the section responsible, within the national police force, for the prior examination of requests for access was functionally independent from the national police in the conduct of its duties and, therefore, satisfied the requirement for a prior review to be carried out by an independent administrative entity. That system of review is complemented by a complaints procedure and by judicial review. Finally, that Member State submits that, if the 2011 Act is ultimately held to be inconsistent with EU law, the temporal effect of any declaration which the referring court makes as a result should be prospective only.  
24      For his part, G.D. submits that the system of general and indiscriminate retention of data established by the 2011 Act and the regime for access to those data provided for by that law are incompatible with EU law as interpreted, in particular, by the Court in paragraph 120 of the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others   
(C-203/15 and C-698/15, EU:C:2016:970).  
25      The referring court states, as a preliminary matter, that it is for it to determine only whether the High Court was correct in law to hold that section 6(1)(a) of the 2011 Act was incompatible with EU law and that, by contrast, the question of the admissibility of the evidence submitted in the context of the criminal proceedings falls within jurisdiction of the Court of Appeal which is seised of the appeal brought against the conviction.  
26      In that context, the referring court has doubts, first of all, as to the requirements of EU law as regards the retention of data for the purposes of combating serious crime. In that regard, it considers, in essence, that only the general and indiscriminate retention of traffic and location data allows serious crime to be combated effectively, which the targeted and expedited retention (  
quick freeze  
) of data does not make possible. As regards targeted retention, the referring court wonders whether it is possible to target specific groups or geographic areas for the purposes of combating serious crimes, since some serious crimes rarely involve circumstances known to the competent national authorities enabling them to suspect the commission of an offence in advance. In addition, targeted retention could give rise to discrimination. As for expedited retention, the referring court considers that that is only useful in situations where it is possible to identify a suspect in the very early stages of an investigation.  
27      As regards, next, access to data retained by providers of electronic communications services, the referring court explains that the national police force established, within its organisation, a system of self-certification of requests addressed to those service providers. Thus, it is clear from the evidence produced before the High Court that the Commissioner of the national police force decided, by an internal measure, that the requests for access made pursuant to the 2011 Act must be dealt with in a centralised manner, by a single national police officer of the rank of Chief Superintendent, namely the head of the security and intelligence section. If that official considers that the data concerned are necessary for the purposes, inter alia, of the prevention, detection, investigation or prosecution of a serious offence, he or she may address a request for access to the providers of electronic communications services. In addition, the Commissioner of the national police force established, within the police force, an independent unit entitled the Telecommunications Liaison Unit (‘the TLU’) in order to provide support to the head of the security and intelligence section in the exercise of his or her duties and to serve as a single point of contact with those service providers.  
28      The referring court adds that, during the period concerned by the criminal investigation brought against G.D., all the requests for access were required to be approved in the first place by a superintendent or inspector acting in that capacity, before they were sent to the TLU to be processed, and that the investigators were directed to include sufficient detail in their requests for access so that an informed decision could be taken. In addition, the TLU and the head of the security and intelligence section were required to examine the legality, necessity and proportionality of requests for access, taking into account the fact that that head could be called upon to answer for his or her decision before the judge designated by the High Court. Furthermore, the TLU is also subject to audit by the Data Protection Commissioner (Ireland).  
29      Finally, the referring court is uncertain as to the scope and temporal effects of a possible declaration of incompatibility of the 2011 Act with EU law. In that regard, it states that such a declaration could only be applied prospectively on the ground the data used as evidence in the criminal proceedings against G.D. were the subject of retention and access at the end of 2013, namely in a period during which Ireland was required to apply the provisions of the 2011 Act transposing Directive 2006/24. According to Ireland, that solution would also be appropriate since, otherwise, the investigation and prosecution of serious offences in Ireland, and the situation of persons already tried and convicted could be seriously impacted.  
30      It was in those circumstances that the Supreme Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is a general/universal data retention regime – even subject to stringent restrictions on retention and access –   
per se  
 contrary to the provisions of Article 15 of Directive [2002/58], interpreted in the light of the Charter?  
(2)      In considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to Directive [2006/24], and making provision for a general data retention regime (subject to the necessary stringent controls on retention and/or in relation to access), and in particular in assessing the proportionality of any such regime, is a national court entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of Directive [2002/58]?  
(3)      In assessing, in the context of determining the compatibility with [EU] law and in particular with Charter Rights of a national measure for access to retained data, what criteria should a national court apply in considering whether any such access regime provides the required independent prior scrutiny as determined by the Court of Justice in its case-law? In that context, can a national court, in making such an assessment, have any regard to the existence of ex post judicial or independent scrutiny?  
(4)      In any event, is a national court obliged to declare the inconsistency of a national measure with the provisions of Article 15 of [Directive 2002/58], if the national measure makes provision for a general data retention regime for the purpose of combating serious crime, and where the national court has concluded, on all the evidence available, that such retention is both essential and strictly necessary to the achievement of the objective of combating serious crime?  
(5)      If a national court is obliged to conclude that a national measure is inconsistent with the provisions of Article 15 of Directive [2002/58], as interpreted in the light of the Charter, is it entitled to limit the temporal effect of any such declaration, if satisfied that a failure to do so would lead to “resultant chaos and damage to the public interest” (in line with the approach taken, for example, in   
R (National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs   
[2018] EWHC 975, at paragraph 46)?  
(6)      May a national court invited to declare the inconsistency of national legislation with Article 15 of [Directive 2002/58], and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 TFEU to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of [Directive 2006/24] issued by the [judgment of 8 April 2014,   
Digital Rights Ireland and Others  
 (C-293/12 and C-594/12, EU:C:2014:238)]?’  
   
Consideration of the questions referred  
   
The first, second and fourth questions  
31      By its first, second and fourth question, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that provides for the general and indiscriminate retention of traffic and location data for the purposes of combating serious crime.  
32      It should be noted, as a preliminary point, that it is settled case-law that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 105 and the case-law cited).  
33      It is clear from the wording itself of Article 15(1) of Directive 2002/58 that the legislative measures that it authorises Member States to take, under the conditions that it lays down, may seek only ‘to restrict the scope’ of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of Directive 2002/58.  
34      As regards the system established by that directive of which Article 15(1) forms part, it must be recalled that, pursuant to the first and second sentences of Article 5(1) of that directive, Member States are required to ensure, through their national legislation, the confidentiality of communications by means of a public communications network and publicly available electronic communications services, as well as of the related traffic data. In particular, they are required to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1) of the same directive.  
35      In that regard, the Court has already held that Article 5(1) of Directive 2002/58 enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires inter alia that, in principle, persons other than users be prohibited from storing, without those users’ consent, those communications and data (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 107).  
36      That provision reflects the objective pursued by the EU legislature when adopting Directive 2002/58. It is apparent from the Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which gave rise to Directive 2002/58, that the EU legislature sought to ‘ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used’. As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of that directive is to protect users of electronic communications services from risks for their personal data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, as stated in recital 2 of the directive, the EU legislature’s intent is to ensure full respect for the rights set out in Articles 7 and 8 of the Charter (see, to that effect, judgments of 21 December 2016,  
 Tele2 Sverige and Watson and Others  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 83, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 106).  
37      In adopting Directive 2002/58, the EU legislature gave concrete expression to those rights, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 109).  
38      As regards the processing and storage by electronic communications service providers of subscribers’ and users’ traffic data, Article 6 of Directive 2002/58 provides, in paragraph 1, that those data must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication, and states, in paragraph 2, that the traffic data necessary for the purposes of subscriber billing and interconnection fees may only be processed up to the end of the period during which the bill may lawfully be challenged or payments pursued in order to obtain payment. As regards location data other than traffic data, Article 9(1) of that directive provides that those data may be processed only subject to certain conditions and after they have been made anonymous or the consent of the users or subscribers obtained.  
39      Therefore, Directive 2002/58 does not merely create a framework for access to such data through safeguards to prevent abuse, but also enshrines, in particular, the principle of the prohibition of their storage by third parties.  
40      In so far as Article 15(1) of Directive 2002/58 permits Member States to adopt legislative measures that ‘restrict the scope’ of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of that directive, such as those arising from the principles of confidentiality of communications and the prohibition on storing related data recalled in paragraph 35 of this judgment, that provision provides for an exception to the general rule provided for inter alia in Articles 5, 6 and 9 and must thus, in accordance with settled case-law, be the subject of a strict interpretation. That provision, therefore, cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of that data, laid down in Article 5 of that directive, to become the rule, if the latter provision is not to be rendered largely meaningless (see, to that effect, judgments of 21 December 2016,  
 Tele2 Sverige and Watson and Others  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 89, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 111).  
41      As regards the objectives that are capable of justifying a limitation of the rights and obligations laid down, in particular, in Articles 5, 6 and 9 of Directive 2002/58, the Court has previously held that the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 112 and the case-law cited).  
42      Furthermore, it is clear from the third sentence in Article 15(1) of Directive 2002/58 that measures taken by the Member States must comply with the general principles of EU law, which include the principle of proportionality, and ensure respect for the fundamental rights guaranteed by the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making them available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 113 and the case-law cited).  
43      Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that that fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 114 and the case-law cited).  
44      It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, first, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing those data, and, second, an interference with the fundamental rights to the respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive, whether the persons concerned have been inconvenienced in any way on account of that interference, or, furthermore, whether the data retained will or will not be used subsequently (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 115 and 116 and the case-law cited).  
45      That conclusion is all the more justified since traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoy special protection under EU law. Taken as a whole, those data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, those data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 117 and the case-law cited).  
46      Therefore, first, the retention of traffic and location data for policing purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of electronic communications systems from exercising their freedom of expression, guaranteed in Article 11 of the Charter, effects that are all the more serious given the quantity and breadth of data retained. Second, in view of the significant quantity of traffic and location data that may be continuously retained under a general and indiscriminate retention measure, as well as the sensitive nature of the information that may be gleaned from those data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 118 and 119 and the case-law cited).  
47      In that regard, it must be emphasised that the retention of and access to those data each constitute, as is clear from the case-law recalled in paragraph 44 of this judgment, separate interferences with the fundamental rights guaranteed by Articles 7 and 11 of the Charter, requiring a separate justification pursuant to Article 52(1) of the Charter. It follows that national legislation ensuring full respect for the conditions established by the case-law interpreting Directive 2002/58 as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference, which results from the general retention of those data provided for under that national legislation, with the rights guaranteed by Articles 5 and 6 of that directive and by the fundamental rights to which those articles give specific effect.  
48      That being said, in so far as Article 15(1) of Directive 2002/58 allows Member States to introduce the derogations referred to in paragraph 34 to 37 of this judgment, that provision reflects the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. Thus, in order to interpret Article 15(1) of Directive 2002/58 in the light of the Charter, account must also be taken of the importance of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter and of the importance of the objectives of protecting national security and combating serious crime in contributing to the protection of the rights and freedoms of others (judgment of 6 October 2020,   
 La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 120 to 122 and the case-law cited).  
49      Thus as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, it should be borne in mind that positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life. Such obligations may also arise from Article 7, concerning the protection of an individual’s home and communications, and Articles 3 and 4, as regards the protection of an individual’s physical and mental integrity and the prohibition of torture and inhuman and degrading treatment (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 126 and the case-law cited).  
50      It is against the backdrop of those different positive obligations that the Court must strike a balance between the various interests and rights at issue. The European Court of Human Rights has held that the positive obligations flowing from Articles 3 and 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, whose corresponding safeguards are set out in Articles 4 and 7 of the Charter, require, in particular, the adoption of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against the person through effective investigation and prosecution, that obligation being all the more important when a child’s physical and moral well-being is at risk. However, the measures to be taken by the competent authorities must fully respect due process and the other safeguards limiting the scope of criminal investigation powers, as well as other freedoms and rights. In particular, according to that court, a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 127 and 128 and the case-law cited).  
51      In that context, it is clear from the wording itself of the first sentence of Article 15(1) of Directive 2002/58 that the Member States may adopt a measure derogating from the principle of confidentiality referred to in paragraph 35 of this judgment where such a measure is ‘necessary, appropriate and proportionate … within a democratic society’, and recital 11 of the directive specifies, in that respect, that a measure of that nature must be ‘strictly’ proportionate to the intended purpose (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 129).  
52      In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130 and the case-law cited).  
53      More specifically, it follows from the Court’s case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 131 and the case-law cited).  
54      In order to satisfy the requirement of proportionality, the national legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subjected to automated processing, in particular where there is a significant risk of unlawful access to those data. Those considerations apply especially where the protection of the particular category of personal data that are sensitive data is at stake (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).  
55      Thus, national legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued. In particular, as regards combating serious crime, the data whose retention is provided for must be capable of contributing to the prevention, detection or prosecution of serious offences (see, to that effect, judgments of 8 April 2014,   
Digital Rights Ireland and Others  
,  
   
C-293/12 and C-594/12, EU:C:2014:238, paragraph 59, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 133).  
56      As regards the public interest objectives that may justify a measure taken pursuant to Article 15(1) of Directive 2002/58, it is clear from the Court’s case-law, in particular the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that, in accordance with the principle of proportionality, there is a hierarchy amongst those objectives according to their respective importance and that the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entails.  
57      In that regard, the Court held that the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU according to which national security remains the sole responsibility of each Member State, exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 and 136).  
58      It is for that reason that the Court held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168).  
59      As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, detecting and prosecuting criminal offences in general (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 140 and the case-law cited).  
60      At the hearing, the European Commission submitted that particularly serious crime could be treated in the same way as a threat to national security.  
61      However, the Court has already held that the objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 135).  
62      It should also be observed that, unlike crime, even particularly serious crime, a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalised and indiscriminate measure of retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 136 and 137).  
63      Thus, criminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. As the Advocate General observed in points 49 to 50 of his Opinion, to treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former.  
64      It also follows that the fact, recalled in the second question referred for a preliminary ruling, that traffic and location data were legally the object of retention for the purpose of safeguarding national security does not have any bearing on the legality of their retention for the purpose of combating serious crime.  
65      As regards the objective of combating serious crime, the Court held that national legislation providing, for that purpose, for the general and indiscriminate retention of traffic and location data exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society. In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of those data is essential for the right to respect for private life. Thus, and also taking into account, first, the dissuasive effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the Charter, referred to in paragraph 46 of this judgment, which is liable to result from the retention of those data, and, second, the seriousness of the interference entailed by such retention, it is necessary, within a democratic society, that retention be the exception and not the rule, as provided for in the system established by Directive 2002/58, and that those data should not be retained systematically and continuously. That conclusion applies even having regard to the objectives of combating serious crime and preventing serious threats to public security and to the importance that must be attached to them (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 141 and 142 and the case-law cited).  
66      In addition, the Court has emphasised that national legislation providing for the general and indiscriminate retention of traffic and location data covers the electronic communications of practically the entire population without any differentiation, limitation or exception being made in the light of the objective pursued. Such legislation is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating serious crime and, in particular, without there being any relationship between the data whose retention is provided for and a threat to public security. In particular, as the Court has already held, such legislation is not restricted to retention in relation to (i) data pertaining to a time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to combating serious crime (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 143 and 144 and the case-law cited).  
67      However, in paragraph 168 of the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), the Court stated that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for  
–        the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;  
–        the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;  
–        the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and  
–        recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (  
quick freeze  
) of traffic and location data in the possession of those service providers,  
provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.  
68      In the present order for reference, which was lodged with the Court before the judgments of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
 (C-746/18, EU:C:2021:152), were delivered, the referring court considered however that only the general and indiscriminate retention of traffic and location data allows serious crime to be combated effectively. At the hearing on 13 September 2021, it was submitted, inter alia by Ireland and the French Government, that that conclusion was not invalidated by the fact that it was possible for the Member States to have recourse to the measures referred to in the preceding paragraph.  
69      In that regard, it must be observed, in the first place, that the effectiveness of criminal proceedings generally depends not on a single means of investigation but on all the means of investigation available to the competent national authorities for those purposes.  
70      In the second place, it must be noted that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by the case-law recalled in paragraph 67 of this judgment, allows Member States to adopt, for the purposes of combating serious crime and preventing serious threats to public security, not only measures for targeted retention and expedited retention, but also measures providing for the general and indiscriminate retention, first, of data relating to the civil identity of users of electronic communications systems and, second, of IP addresses assigned to the source of a connection.  
71      In that respect, it is common ground that retention of data relating to the civil identity of users of electronic communications systems may contribute to the fight against serious crime to the extent that those data make it possible to identify persons who have used those means in the context of planning or committing an act constituting serious crime.  
72      As is clear from the case-law summarised in paragraph 67 of this judgment, Directive 2002/58 does not preclude, for the purposes of combating crime in general, the general retention of data relating to civil identity. In those circumstances, it must be stated that neither the directive nor any other EU law act precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser’s identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities.  
73      In addition, it should be recalled that the generalised retention of IP addresses of the source of connection constitutes a serious interference in the fundamental rights enshrined in Articles 7 and 8 of the Charter as those IP addresses may allow precise conclusions to be drawn concerning the private life of the user of the means of electronic communication concerned and may be a deterrent to the exercise of freedom of expression guaranteed in Article 11 of the Charter. However, as regards such retention, the Court has held that in order to strike the necessary balance between the rights and interests at issue as required by the case-law referred to in paragraphs 50 to 53 of this judgment, it is necessary to take into account, in a case of an offence committed online and, in particular, in cases of the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1), the fact that the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 153 and 154).  
74      Hence, the Court held that such general and indiscriminate retention solely of IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of those data, as referred to in paragraphs 155 and 156 of the judgment of 6 October 2020,   
La Quadrature du Net and Others   
(C-511/18, C-512/18 and C-520/18, EU:C:2020:791).  
75      In the third place, as regards legislative measures providing for a targeted retention and an expedited retention of traffic and location data, the indications provided in the order for reference show a narrower understanding of the scope of those measures than that upheld in the case-law recalled in paragraph 67 of this judgment. While, as is recalled in paragraph 40 of this judgment, those retention measures are a derogation within the system established by Directive 2002/58, that directive, read in the light of the fundamental rights enshrined in Articles 7, 8 and 11 and Article 52(1) of the Charter, does not make the possibility of issuing an order requiring a targeted retention subject to the condition either that the places likely to be the location of a serious crime or the persons suspected of being involved in such an act must be known in advance. Likewise, that directive does not require that the order requiring an expedited retention be limited to suspects identified in advance of that order.  
76      As regards, first, targeted retention, the Court held that Article 15(1) of Directive 2002/58 does not preclude national legislation based on objective evidence which makes it possible to target persons whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security (judgments of 21 December 2016,  
 Tele2 Sverige and Watson and Others  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 148).  
77      The Court stated, in that regard, that, while the objective evidence may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective and non-discriminatory factors, as posing a threat to public or national security in the Member State concerned (see, to that effect, judgments of 21 December 2016,   
Tele2 Sverige and Watson and Others  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 110, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 149).  
78      Member States thus have, inter alia, the option of imposing retention measures targeting persons who, on the basis of an identification, are the subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending. Where that identification is based on objective and non-discriminatory factors, defined in national law, targeted retention in respect of persons thus identified is justified.  
79      Second, a targeted measure for the retention of traffic and location data may, at the choice of the national legislature and in strict compliance with the principle of proportionality, also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to serious crime, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 150 and the case-law cited).  
80      It should be borne in mind that, according to that case-law, the competent national authorities may adopt, for areas referred to in the preceding paragraph, a targeted measure of retention using a geographic criterion, such as, inter alia, the average crime rate in a geographical area, without that authority necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime. Since a targeted retention using that criterion is likely to concern, depending on the serious criminal offences in question and the situation specific to the respective Member States, both the areas marked by a high incidence of serious crime and areas particularly vulnerable to the commission of those acts, it is, in principle, not likely moreover to give rise to discrimination, as the criterion drawn from the average rate of serious crime is entirely unconnected with any potentially discriminatory factors.  
81      In addition and above all, a targeted measure of retention covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect traffic data and, in particular, location data of all persons using, at a specific time, a means of electronic communication in one of those places. Thus, such a targeted retention measure may allow those authorities to obtain, through access to the retained data, information as to the presence of those persons in the places or geographical areas covered by that measure as well as their movements between or within those areas and to draw, for the purposes of combating serious crime, conclusions as to their presence and activity in those places or geographical areas at a specific time during the period of retention.  
82      It should also be noted that the geographic areas covered by such a targeted retention measure may and, where appropriate, must be amended in accordance with changes in the circumstances that justified their selection, thus making it possible to react to developments in the fight against serious crime. The Court has held that the duration of those targeted retention measures described in paragraphs 76 to 81 of this judgment must not exceed what is strictly necessary in the light of the objective pursued and the circumstances justifying them, without prejudice to the possibility of extending those measures should such retention continue to be necessary (judgment of 6 October 2020,  
 La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 151).  
83      As regards the possibility of providing distinctive criteria other than a personal or geographic criterion for the targeted retention of traffic and location data, it is possible that other objective and non-discriminatory criteria may be considered in order to ensure that the scope of a targeted retention measure is as limited as is strictly necessary and to establish a connection, at least indirectly, between serious criminal acts and the persons whose data are retained. However, since Article 15(1) of Directive 2002/58 refers to legislative measures of the Member States, it is for the latter and not for the Court to identify those criteria, it being understood that there can be no question of reinstating, by that means, the general and indiscriminate retention of traffic and location data.  
84      In any event, as Advocate General Campos Sánchez-Bordona observed in point 50 of his Opinion in Joined Cases   
SpaceNet and Telekom Deutschland   
(C-793/19 and C-794/19, EU:C:2021:939), the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general retention of traffic and location data.  
85      As regards, second, the expedited retention of traffic and location data processed and stored by providers of electronic communications services on the basis of Articles 5, 6 and 9 of Directive 2002/58 or on the basis of legislative measures taken under Article 15(1) of that directive, it should be noted that those data must, in principle, be erased or made anonymous, depending on the circumstances, at the end of the statutory periods within which those data must be processed and stored in accordance with the national provisions transposing that directive. Nevertheless, the Court has held that during that processing and storage, situations may arise in which it becomes necessary to retain those data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may reasonably be suspected (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 160 and 161).  
86      In such a situation, in the light of the balance that must be struck between the rights and interests at issue referred to in paragraphs 50 to 53 of this judgment, it is permissible for Member States to provide, in legislation adopted pursuant to Article 15(1) of Directive 2002/58, for the possibility of instructing, by means of a decision of the competent authority subject to effective judicial review, providers of electronic communications services to undertake the expedited retention of traffic and location data at their disposal for a specified period of time (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 163).  
87      To the extent that the purpose of that expedited retention no longer corresponds to the purpose for which those data were initially collected and retained and since any processing of data must, under Article 8(2) of the Charter, be consistent with specified purposes, Member States must make clear, in their legislation, for what purpose the expedited retention of data may occur. In the light of the serious nature of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter which such retention may entail, only actions to combat serious crime and, a fortiori, to safeguard national security are such as to justify such interference, on the condition that the measure and access to the retained data comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).  
88      The Court has stated that a measure of retention of that nature need not be limited to the data of persons who have been identified previously as being a threat to public security or national security of the Member State concerned or of persons specifically suspected of having committed a serious criminal offence or acts adversely affecting national security. According to the Court, while it must comply with the framework established by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, and taking into account the findings in paragraph 55 of this judgment, such a measure may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that those data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, and his or her social or professional circle (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 165).  
89      Thus, a legislative measure may authorise the issuing of an instruction to providers of electronic communications services to carry out the expedited retention of traffic and location data, inter alia, of persons with whom, prior to the serious threat to public security arising or a serious crime being committed, a victim was in contact via those electronic means of communications.  
90      Such expedited retention may, according to the Court’s case-law recalled in paragraph 88 of this judgment and under the same conditions as those referred to in that paragraph, also be extended to specific geographic areas, such as the places of the commission of or preparation for the offence or attack on national security in question. It should be stated that the subject matter of such a measure may also be the traffic and location data relating to a place or a person, possibly the victim of a serious crime, who has disappeared, on condition that that measure and access to the data so retained comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020,  
 La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).  
91      Furthermore, it must be stated that Article 15(1) of Directive 2002/58 does not preclude the competent national authorities from ordering a measure of expedited retention at the first stage of an investigation into a serious threat for public security or a possible serious crime, namely from the time when the authorities may, in accordance with the provisions of national law, commence such an investigation.  
92      As regards the variety of measures for the retention of traffic and location data referred to in paragraph 67 of this judgment, it must be stated that those various measures may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently. Accordingly, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by case-law resulting from the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), does not preclude a combination of those measures.  
93      In the fourth and final place, it must be emphasised that the proportionality of the measures adopted pursuant to Article 15(1) of Directive 2002/58 requires, according to the Court’s settled case-law, as recalled in the judgment of 6 October 2020,  
 La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), compliance not only with the requirements of aptitude and of necessity but also with that of the proportionate nature of those measures in relation to the objective pursued.  
94      In that context, it should be recalled that, in paragraph 51 of its judgment of 8 April 2014,   
Digital Rights Ireland and Others   
(C-293/12 and C-594/12, EU:C:2014:238), the Court held that while the fight against serious crime is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques, that objective of general interest, however fundamental it may be, does not, in itself, justify that a measure providing for the general and indiscriminate retention of all traffic and location data, such as that established by Directive 2006/24, should be considered to be necessary.  
95      In the same vein, the Court stated, in paragraph 145 of the judgment of 6 October 2020,   
La Quadrature du Net and Others   
(C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that even the positive obligations of the Member States which may arise, depending on the circumstances, from Articles 3, 4 and 7 of the Charter and which relate, as pointed out in paragraph 49 of this judgment, to the establishment of rules to facilitate effective action to combat criminal offences, cannot have the effect of justifying interference that is as serious as that entailed by legislation providing for the retention of traffic and location data with the fundamental rights, enshrined in Articles 7 and 8 of the Charter, of practically the entire population, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued.  
96      At the hearing, the Danish Government submitted that the competent national authorities should be able to access, for the purpose of fighting serious crime, traffic and location data which have been retained in a general and indiscriminate way, in accordance with the line of case-law resulting from the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 to 139), in order to address a serious threat to national security that is genuine and present, or foreseeable.  
97      It should be observed, first of all, that the fact of authorising access for the purpose of combating serious crime to traffic and location data which have been retained in a general and indiscriminate way would make that access depend upon facts that fall outside that objective, according to whether or not, in the Member State concerned there was a serious threat to national security as referred to in the preceding paragraph, whereas, in view of the sole objective of the fight against serious crime which must justify the retention of those data and access thereto, there is nothing to justify a difference in treatment, in particular, as between the Member States.  
98      As the Court has already held, access to traffic and location data retained by providers in accordance with a measure taken under Article 15(1) of Directive 2002/58, which must be given effect in full compliance with the conditions resulting from the case-law interpreting Directive 2002/58, may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data. It is otherwise only if the importance of the objective pursued by access is greater than that of the objective which justified retention (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 165 and 166).  
99      The Danish Government’s submission refers to a situation in which the objective pursued by the access request proposed, namely the fight against serious crime, is of lesser importance in the hierarchy of objectives of public interest than that which justified the retention, namely the safeguarding of national security. To authorise, in that situation, access to retained data would be contrary to that hierarchy of public interest objectives recalled in the preceding paragraph, and also to paragraphs 53, 56, 57 and 59 of this judgment.  
100    In addition and moreover, in accordance with the case-law recalled in paragraph 65 of this judgment, traffic and location data cannot be the object of general and indiscriminate retention for the purpose of combating serious crime and, therefore, access to those data cannot be justified for that same purpose. Where those data have exceptionally been retained in a general and indiscriminate way for the purpose of the safeguarding of national security against a genuine and present or foreseeable threat, in the circumstances referred to in paragraph 58 of this judgment, the national authorities competent to undertake criminal investigations cannot access those data in the context of criminal proceedings, without depriving of any effectiveness the prohibition on such retention for the purpose of combating serious crime, recalled in paragraph 65.  
101    In the light of all of the foregoing considerations, the answer to the first, second and fourth questions is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which provide, as a preventive measure, for the purposes of combating serious crime and for the prevention of serious threats to public security, for the general and indiscriminate retention of traffic and location data. However, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that, for the purposes of combating serous crime and preventing serious threats to public security, provide for:  
–        the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;  
–        the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;  
–        the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and  
–        recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,  
provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.  
   
The third question  
102    By its third question, the referring court asks, in essence, whether, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to retained data, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, assisted by a unit established within the police service which enjoys a degree of autonomy in the exercise of its duties and whose decisions may subsequently by subject to judicial review.  
103    As a preliminary matter, it should be borne in mind that, while it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to data in their possession, the national legislation must, in order to satisfy the requirement of proportionality, as recalled in paragraph 54 of this judgment, lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse (see, to that effect, judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
,   
 C-746/18, EU:C:2021:152, paragraph 48 and the case-law cited).  
104    In particular, national legislation governing the access by the competent authorities to retained traffic and location data, adopted pursuant to Article 15(1) of Directive 2002/58, cannot be limited to requiring that the authorities’ access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 49 and the case-law cited).  
105    Accordingly, since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that those data might, in a specific case, make an effective contribution to combating such activities (judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
,   
 C-746/18, EU:C:2021:152, paragraph 50 and the case-law cited).  
106    In order to ensure, in practice, that those conditions are fully observed, it is essential that access by the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 51 and the case-law cited).  
107    One of the requirements for the prior review is that the court or independent administrative body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 52).  
108    Where that review is carried out not by a court but by an independent administrative body, that body must have a status that enables it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence. Accordingly, it follows that the requirement of independence that has to be satisfied by the body entrusted with carrying out the prior review means that that body must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the body entrusted with the prior review, first, should not be involved in the conduct of the criminal investigation in question and, second, must have a neutral stance vis-à-vis the parties to the criminal proceedings (see, to that effect, judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
,   
 C-746/18, EU:C:2021:152, paragraphs 53 and 54).  
109    Thus, the Court has, inter alia, found that a public prosecutor’s office, which directs the investigation procedure and, where appropriate, brings the public prosecution cannot be considered to have third party status in relation to the interests at issue, since it has the task not of ruling on a case in complete independence but, acting as prosecutor in the proceedings, of bringing it, where appropriate, before the court that has jurisdiction. Consequently, a public prosecutor’s office is not in a position to carry out the prior review of requests for access to retained data (see, to that effect, judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraphs 55 and 57).  
110    Finally, the independent review required in accordance with Article 15(1) of Directive 2002/58 must take place before any access to the data concerned, except in the event of duly justified urgency, in which case the review must take place within a short time. A subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met (see, to that effect, judgments of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 189, and of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 58).  
111    In the present case, it is apparent from the order for reference that the 2011 Act assigns to a police officer, whose rank is not below that of chief superintendent, the power to carry out the prior review of requests for access to data issued by the police investigation services and to request the providers of electronic communications services to transmit the data that they retain to those services. To the extent that that officer does not have the status of a third party in relation to those services, he or she does not fulfil the requirements for independence and impartiality recalled in paragraph 108 of this judgment, notwithstanding the fact that he or she is assisted in that duty by a police unit, in this case the TLU, which benefits from a certain degree of autonomy in the exercise of its duties.  
112    Next, while it is true that the 2011 Act provides for mechanisms of review subsequent to the decision of the competent police officer in the form of a complaint procedure and a procedure before a judge responsible for examining the application of the provisions of that act, it is clear from the case-law recalled in paragraph 110 of this judgment that a review carried out subsequently cannot be substituted for the requirement, recalled in paragraph 106 of this judgment, for a review that is independent and, except in duly justified urgent cases, undertaken beforehand.  
113    Finally, the 2011 Act does not lay down any objective criteria which define precisely the conditions and circumstances in which national authorities must be granted access to data and the police officer responsible for processing the requests for access to retained data is solely competent, as Ireland confirmed at the hearing, to assess the suspicions that exist with respect to the persons concerned and the need for access to data that relate to them.  
114    Consequently, the answer to the third question is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to data retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.  
   
The fifth and sixth questions  
115    By its fifth and sixth questions, which it is appropriate to examine together, the referring courts asks, in essence, whether EU law must be interpreted as meaning that a national court may limit the temporal effects of a declaration of invalidity which it is required to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58 read in the light of the Charter.  
116    It is apparent from the information provided by the referring court that the national legislation at issue in the main proceedings, namely the 2011 Act, was adopted in order to transpose into national law Directive 2006/24, which was later declared invalid by the Court in its judgment of 8 April 2014,   
Digital Rights Ireland and Others   
(C-293/12 and C-594/12, EU:C:2014:238).  
117    In addition, the referring court states that, while the assessment of the admissibility of the evidence based on data retained pursuant to the 2011 Act and relied on as regards G.D. in the context of the criminal proceedings is a matter for the criminal court, it is nevertheless, in the context of the civil proceedings, its responsibility to rule on the validity of the provisions at issue of that act and on the temporal effects of a declaration of invalidity of those provisions. Thus, while the sole issue raised before the referring court is that of the validity of the provisions of the 2011 Act, that court considers however that it is necessary to inquire of the Court as to the effect of a possible finding of invalidity on the admissibility of the evidence obtained by means of the general and indiscriminate retention of data that that act permitted.  
118    In the first place, it should be recalled that the principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State bodies to give full effect to the various provisions of EU law, and the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States. In the light of that principle, where it is unable to interpret national legislation in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means (see, to that effect, judgments of 15 July 1964,   
Costa  
, 6/64, EU:C:1964:66, p. 594; of 19 November 2019,   
A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)  
, C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraphs 157, 158 and 160; and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 214 and 215).  
119    Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested. The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (judgment of 6 October 2020,  
 La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 216 and 217 and the case-law cited).  
120    It is true that the Court has held, in a case concerning the lawfulness of measures adopted in breach of the obligation under EU law to conduct a prior assessment of the impact of a project on the environment and on a protected site, that if domestic law allows it, a national court may, by way of exception, maintain the effects of such measures where such maintenance is justified by overriding considerations relating to the need to nullify a genuine and serious threat of interruption in the electricity supply in the Member State concerned, which cannot be remedied by any other means or alternatives, particularly in the context of the internal market, and continues only for as long as is strictly necessary to remedy the breach (see, to that effect, judgment of 29 July 2019,   
Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen  
, C-411/17, EU:C:2019:622, paragraphs 175, 176, 179 and 181).  
121    However, unlike a breach of a procedural obligation such as the prior assessment of the impact of a project in the specific field of environmental protection, a failure to comply with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure referred to in the preceding paragraph (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 219).  
122    Maintaining the effects of national legislation such as the 2011 Act would mean that the legislation would continue to impose on providers of electronic communications services obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data have been retained (see, by analogy, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 219).  
123    Therefore, the referring court cannot limit the temporal effects of a declaration of invalidity which it is bound to make under national law in respect of the national legislation at issue in the main proceedings (see, by analogy, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 220).  
124    In that regard, as the Advocate General observed in essence in point 75 of his Opinion, the fact that that legislation was adopted in order to transpose Directive 2006/24 into national law is irrelevant since, due to the Court’s decision that that directive was invalid, the invalidity has effect as from the date of its entry into force (see, to that effect, judgment of 8 February 1996,  
 FMC and Others  
, C-212/94, EU:C:1996:40, paragraph 55), the validity of that national legislation must be assessed by the referring court in the light of Directive 2002/58 and the Charter, as interpreted by the Court.  
125    As regards, more specifically, the interpretation of Directive 2002/58 and the Charter upheld by the Court in its judgments of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), and of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), it should be recalled that, according to settled case-law, the interpretation that the Court gives to a rule of EU law, in the exercise of the jurisdiction conferred upon it by Article 267 TFEU, clarifies and defines the meaning and scope of that rule as it must be, or ought to have been, understood and applied from the time of its coming into force. It follows that the rule as thus interpreted may and must be applied by the courts to legal relationships arising and established before the judgment ruling on the request for interpretation, provided that in other respects the conditions for bringing an action relating to the application of that rule before the courts having jurisdiction are satisfied (judgment of 16 September 2020,   
Romenergo and Aris Capital  
, C-339/19, EU:C:2020:709, paragraph 47 and the case-law cited).  
126    In that regard, it should also be stated that a temporal limitation of the effects of the interpretation given was not imposed in the judgments of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), and of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), with the result that, in accordance with the case-law recalled in paragraph 119 of this judgment, it should not be imposed in a judgment of the Court subsequent to those judgments.  
127    Finally, as regards the effect of a declaration of the potential incompatibility of the 2011 Act with Directive 2002/58, read in the light of the Charter, on the admissibility of evidence relied on against G.D. in the context of the criminal proceedings, it suffices to refer to the Court’s case-law on that subject, in particular the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
 (C-746/18, EU:C:2021:152), from which it follows that that admissibility is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.  
128    Having regard to the foregoing considerations, the answer to the fifth and sixth questions is that EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of invalidity which it is bound to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58 read in the light of the Charter. The admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member State, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.  
   
Costs  
129    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding legislative measures which, as a preventive measure for the purposes of combating serious crime and preventing serious threats to public security, provide for the general and indiscriminate retention of traffic and location data. However, that Article 15(1), read in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights, does not preclude legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for  
–          
the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;  
–          
the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;  
–          
the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and  
–          
recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,  
provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.  
2.        
Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to data, which have been retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.  
3.        
EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of invalidity which it is bound to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of the Charter of Fundamental Rights. The admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.  
Lenaerts  
Arabadjiev  
Prechal  
Rodin  
Jarukaitis  
Jääskinen  
von Danwitz  
Safjan   
Biltgen  
Xuereb  
Piçarra  
Rossi  
   
      Kumin        
   
Delivered in open court in Luxembourg on 5 April 2022.  
A. Calot Escobar  
   
K. Lenaerts  
Registrar  
   
President  
\*      Language of the case: English.  
   
  
  
  
  
Disclaimer

ID: 4953dc82-2975-441a-85c8-342b1cc14a93

of 20 Oct 2022, C-306/21 (  
Koalitsia Demokratichna Bulgaria - Obedinenie  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material scope - Activity outside the scope of Union law exemption   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Powers   
   
JUDGMENT OF THE COURT (Eighth Chamber)  
20 October 2022 (\*)  
(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Scope – Article 2(2)(a) – Concept of ‘activity which falls outside the scope of Union law’ – National and European elections – Article 6(1)(e) – Lawfulness of processing – Article 58 – Measure adopted by the supervisory authorities which limits or, where appropriate, prohibits the video recording of the vote count at polling stations)  
In Case C-306/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Varhoven administrativen sad (Supreme Administrative Court, Bulgaria), made by decision of 23 April 2021, received at the Court on 12 May 2021, in the proceedings  
Komisia za zashtita na lichnite danni,  
Tsentralna izbiratelna komisia  
v  
Koalitsia ‘Demokratichna Bulgaria – Obedinenie’,  
THE COURT (Eighth Chamber),  
composed of N. Piçarra, acting as President of the Chamber, N. Jääskinen (Rapporteur) and M. Gavalec, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        the Komisia za zashtita na lichnite danni, by V. Karadzhov,  
–        the Romanian Government, by L.-E. Baţagoi, E. Gane and A. Wellman, acting as Agents,  
–        the European Commission, by A. Bouchagiar, C. Georgieva and H. Kranenborg, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2(2)(a) and Article 6(1)(e) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
2        The request has been made in proceedings between, on the one hand, the Komisia za zashtita na lichnite danni (Commission for the Protection of Personal Data, Bulgaria) (‘the CPPD’) and the Tsentralna izbiratelna komisia (Central Election Commission, Bulgaria) (‘the CEC’) and, on the other hand, the Koalitsia ‘Demokratichna Bulgaria – Obedinenie’ (‘the Koalitsia’), a coalition of Bulgarian political parties, concerning guidelines on the processing and protection of personal data in the electoral process (‘the guidelines at issue’), adopted by the CPPD and the CEC.  
   
Legal framework  
   
E  
uropean   
U  
nion  
 law  
3        Recitals 4, 16 and 129 of the GDPR are worded as follows:  
‘(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the [Charter of Fundamental Rights of the European Union] as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.  
…  
(16)      This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the [European] Union.  
…  
(129)      In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers … Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing … In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation …’  
4        Article 2 of that regulation, entitled ‘Material scope’, provides:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the [EU Treaty];  
…’  
5        Article 3 of that regulation defines its territorial scope. According to paragraph 1 thereof, the GDPR ‘applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not’.  
6        According to Article 4 of the GDPR:  
‘For the purposes of this Regulation:  
…  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…’  
7        Article 5 of that regulation, entitled ‘Principles relating to processing of personal data’, provides:  
‘1.      Personal data shall be:  
…  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
…’  
8        Article 6 of that regulation, entitled ‘Lawfulness of processing’, provides in paragraphs 1 to 3 thereof:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
…  
2.      Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.  
3.      The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.  
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.’  
9        Article 58 of that regulation, entitled ‘Powers’, provides in paragraphs 2 to 4 thereof:  
‘2.      Each supervisory authority shall have all of the following corrective powers:  
…  
(f)      to impose a temporary or definitive limitation including a ban on processing;  
…  
3.      Each supervisory authority shall have all of the following authorisation and advisory powers:  
…  
(b)      to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;  
…  
4.      The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the [Charter of Fundamental Rights].’  
10      As set out in Article 85 of the GDPR, entitled ‘Processing and freedom of expression and information’:  
‘1.      Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.  
2.      For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.  
3.      Each Member State shall notify to the [European] Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.’  
   
Bulgarian law  
11      Article 272 of the Izboren kodeks (Electoral Code), in the version applicable to the dispute in the main proceedings, provides:  
‘When the ballot boxes are opened and the results of the voting are determined, candidates, supporters and representatives of parties, coalitions and action committees …, observers …, one registered researcher for each registered sociological research agency and representatives of the media may be present at polling stations and must be provided with a direct view of the vote count.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
12      The guidelines at issue were adopted by decision of the CPPD on 28 January 2021 and by decision of the CEC on 8 February 2021.  
13      As regards the processing of personal data by means of video recording (recording or live broadcast) in the context of the electoral process, the guidelines at issue provide that the purpose of such processing is to ensure the transparency, objectivity and lawfulness of the electoral process, as well as the equal treatment of participants in that process, and to guarantee freedom of expression and the right to information.  
14      As regards the detailed arrangements for processing personal data by means of video recording during the electoral process, the guidelines at issue provide, on the one hand, that the media are to process personal data by means of video recording only when the election day starts and concludes, when the results of the voting are announced and when the serial numbers of the ballot papers are drawn.  
15      On the other hand, those guidelines state that no other participants in the electoral process may process personal data by means of video recording, since this would be incompatible with their role in the electoral process.  
16      By application of 10 February 2021, the Koalitsia contested the lawfulness of those guidelines before the Administrativen sad Sofia (Administrative Court, Sofia, Bulgaria) in so far as they apply to the processing of personal data by means of video recording.  
17      By judgment of 15 March 2021, that court annulled:  
–        paragraph 2 of Section I of the guidelines at issue, entitled ‘General considerations’, in so far as it concerns controllers, processors and persons who process personal data in the context of an electoral process in accordance with the controller’s instructions and which provides that ‘their rights and obligations with regard to the processing of personal data are limited in so far as their rights and obligations in the context of the electoral process are exhaustively and restrictively set out’, that ‘the cases in which those persons process personal data are expressly set out in the Electoral Code (right to a direct view when results of the voting are determined, right to obtain copies of the reports of the district electoral commission, etc.)’, and that ‘when processing personal data, those persons may not go beyond the rights and obligations provided for in the Electoral Code’; and  
–        paragraph 9 of Section II, entitled ‘Guidelines for data controllers’, in so far as that paragraph provides that ‘no other participants in the electoral process may process personal data by means of video recording and/or dissemination, because their role in the electoral process is incompatible with the objective of processing personal data in the electoral process by means of video recording’ and that ‘the tasks and roles of those participants in the electoral process are expressly and exhaustively defined in the Electoral Code’.  
18      According to the Administrativen sad Sofia (Administrative Court, Sofia), under Article 2(2)(a) of the GDPR, that regulation does not apply in the course of an activity which falls outside the scope of EU law, such as that at issue in the main proceedings, that is to say, the organisation of national parliamentary or local authority elections in a Member State. Consequently, the guidelines at issue, in so far as they are measures implementing the GDPR, have no legal basis.  
19      On 29 March 2021, the CPPD and the CEC appealed against that judgment to the Varhoven administrativen sad (Supreme Administrative Court, Bulgaria), the referring court.  
20      By application of 2 April 2021, the CPPD, supported by the CEC, requested that a preliminary ruling be sought from the Court of Justice concerning the applicability of EU law to the case in the main proceedings.  
21      The Koalitsia argues before the referring court that that judgment should be upheld and that there is no need to submit a request for a preliminary ruling to the Court of Justice.  
22      The referring court states that the guidelines at issue constitute an administrative measure which has recurring legal effects during elections. It points out that the guidelines at issue apply to all national, local and European elections held on the territory of the Republic of Bulgaria.  
23      That court is uncertain, in particular, as to the applicability of the GDPR in the context of the organisation of elections in a Member State and, in the event that it is applicable in that context, as to the impact of the provisions of the GDPR on the ability of the competent personal data protection authorities to limit or, where appropriate, to prohibit the processing of such data in the context of the electoral process.  
24      In those circumstances, the Varhoven administrativen sad (Supreme Administrative Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 2(2)(a) of the [GDPR] to be interpreted as precluding the application of that regulation to an ostensibly purely internal situation, such as the holding of elections to the National Assembly, where the subject matter of the protection is the personal data of individuals – citizens of the European Union – and the data processing operations are not restricted to the collection of data in the context of the activity in question?  
(2)      If the first question is answered in the affirmative, does the conclusion of the holding of elections to the National Assembly, which do not appear to fall within the scope of EU law, release controllers, processors and persons who store personal data from their obligations under the regulation, as the sole means of protecting personal data of EU citizens at EU level? Does the applicability of the regulation depend solely on the activity for which the personal data were produced or collected, thereby also leading to the conclusion that its subsequent applicability is precluded?  
(3)      If the first question is answered in the negative, do Article 6[(1)](e) of the [GDPR] and the principle of proportionality enshrined in recitals 4 and 129 thereof preclude national rules implementing the regulation, such as those at issue, which preclude and restrict from the outset the possibility of carrying out any video recording during the determination of the election results at polling stations, do not allow for differentiation and regulation of individual elements of the recording process and preclude the possibility of achieving the objectives of the regulation – the protection of personal data of individuals – by other means?  
(4)      Alternatively, and in the context of the scope of application of EU law, do Article 6[(1)](e) of the [GDPR] and the principle of proportionality enshrined in recitals 4 and 129 thereof preclude – in the holding of municipal elections and elections to the European Parliament – national rules implementing that regulation, such as those at issue, which preclude and restrict from the outset the possibility of carrying out any video recording during the determination of the election results at polling stations, do not differentiate and regulate individual elements of the recording process or even allow for such differentiation and regulation, and preclude the possibility of achieving the objectives of the regulation – the protection of personal data of individuals – by other means?  
(5)      Does Article 6(1)(e) of the [GDPR] preclude the categorisation of the activities of ascertaining lawful conduct and determining the results of elections as a task carried out in the public interest which justifies a certain degree of interference, subject to the requirement of proportionality, with regard to the personal data of persons present at polling stations when they perform an official, public task which is regulated by law?  
(6)      If the previous question is answered in the affirmative, does the protection of personal data preclude the introduction of a national statutory prohibition on the collection and processing of personal data, which limits the possibility of carrying out ancillary activities consisting in the video recording of materials, objects or items which do not contain personal data, where the recording process potentially gives rise to the possibility of personal data also being collected during the video recording of persons present at polling stations who are carrying out an activity in the public interest at the relevant time?’  
   
The admissibility of the request for a preliminary ruling  
25      On 14 September 2021, the Court sent a request for information to the referring court, asking it to clarify whether the amendment of Article 272 of the Electoral Code, which occurred after the request for a preliminary ruling was lodged, had any impact on the relevance of the questions referred for the resolution of the dispute in the main proceedings.  
26      In its reply of 29 October 2021, the referring court stated that, under national procedural law, it must assess the legality of the guidelines at issue by reference not to the date on which that legislative amendment was made, but to the date on which the guidelines at issue were adopted. Consequently, the relevance of the reference for a preliminary ruling is not called into question by that legislative amendment, which took place after the adoption of the guidelines at issue.  
27      In that regard, it should be noted that, according to the settled case-law of the Court, questions referred for a preliminary ruling by a national court in the legislative and factual context which that court is responsible for defining, and the accuracy of which is not a matter for the Court of Justice to determine, enjoy a presumption of relevance. The Court may refuse to give a ruling on a question referred by a national court for a preliminary ruling, under Article 267 TFEU, only where, for instance, the requirements concerning the content of a request for a preliminary ruling, set out in Article 94 of the Rules of Procedure of the Court, are not satisfied or where it is quite obvious that the interpretation of a provision of EU law, or the assessment of its validity, which is sought by the national court, bears no relation to the actual facts of the main action or to its purpose, or where the problem is hypothetical (judgment of 25 March 2021,   
Obala i lučice  
, C-307/19, EU:C:2021:236, paragraph 48 and the case-law cited).  
28      In the present case, it is clear from the explanations given by the referring court that it considers that the response to the questions raised is necessary for it to rule on the dispute before it.  
29      It follows that the request for a preliminary ruling is admissible.  
   
The questions referred for a preliminary ruling  
   
The first and second questions  
30      By its first and second questions, which it is appropriate to consider together, the referring court asks, in essence, whether Article 2(2)(a) of the GDPR must be interpreted as excluding from the scope of that regulation the processing of personal data in the context of the organisation of elections in a Member State.  
31      First, it should be noted that, pursuant to Article 2(1) of the GDPR, that regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. According to Article 4(2) of that regulation, the definition of ‘processing’ includes any operation which is performed on personal data or on sets of personal data, whether or not by automated means, such as, inter alia, collection, recording, use, disclosure by transmission, dissemination or otherwise making available.  
32      It follows that the video recording of natural persons amounts to a processing of personal data which falls, in principle, within the material scope of the GDPR (see, to that effect, judgment of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraph 35).  
33      Secondly, it should be pointed out that the exceptions to the material scope of that regulation are exhaustively set out in Article 2(2) and (3) of that regulation.  
34      In the present case, the referring court is uncertain as to whether the processing of personal data by means of video recording during the organisation of both European and national elections falls within the exception provided for in Article 2(2)(a) of the GDPR, according to which that regulation does not apply to the processing of personal data ‘in the course of an activity which falls outside the scope of Union law’.  
35      It must be pointed out that that exception to the applicability of the GDPR must, like the other exceptions laid down in Article 2(2), be interpreted strictly (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 62 and the case-law cited).  
36      As the Court has held, Article 2(2)(a) of the GDPR is to be read in conjunction with Article 2(2)(b) thereof and recital 16, which states that that regulation does not apply to the processing of personal data in the context of ‘activities which fall outside the scope of Union law, such as activities concerning national security’ and ‘activities in relation to the common foreign and security policy of the Union’ (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 63).  
37      It follows that Article 2(2)(a) and (b) of the GDPR represents partly a continuation of the first indent of Article 3(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31). Therefore, Article 2(2)(a) and (b) of the GDPR cannot be interpreted in broader terms than the exception resulting from the first indent of Article 3(2) of Directive 95/46, a provision which already excluded from that directive’s scope inter alia the processing of personal data taking place in the course ‘of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the [EU Treaty, in the version in force prior to the Treaty of Lisbon,] and in any case … processing operations concerning public security, defence, State security …’ (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 64).  
38      However, only the processing of personal data in the course of an activity of the State or of State authorities which was expressly listed in Article 3(2) of Directive 95/46 or in the course of an activity which could be classified in the same category was excluded from the scope of that directive (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 65 and the case-law cited).  
39      Therefore, Article 2(2)(a) of the GDPR, read in the light of recital 16 thereof, is designed solely to exclude from the scope of that regulation the processing of personal data carried out by State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category, with the result that the mere fact that an activity is an activity characteristic of the State or of a public authority is not sufficient ground for that exception to be automatically applicable to such an activity (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 66 and the case-law cited).  
40      The activities having the aim of safeguarding national security that are envisaged in Article 2(2)(a) of the GDPR encompass, in particular, those that are intended to protect essential State functions and the fundamental interests of society (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 67).  
41      However, activities relating to the organisation of elections in a Member State do not pursue such an objective and consequently cannot be classified in the category of activities having the aim of safeguarding national security, which are envisaged in Article 2(2)(a) of the GDPR.  
42      In the light of the foregoing considerations, the answer to the first and second questions is that Article 2(2)(a) of the GDPR must be interpreted as not excluding from the scope of that regulation the processing of personal data in the context of the organisation of elections in a Member State.  
   
The third to sixth questions  
43      First of all, it should be observed that, according to settled case-law, in the procedure laid down in Article 267 TFEU providing for cooperation between national courts and the Court of Justice, it is for the latter to provide the national court with an answer which will be of use to it and enable it to determine the case before it. To that end, the Court may have to reformulate the questions referred to it (see, to that effect, judgment of 7 July 2022,   
Pensionsversicherungsanstalt (Child-raising periods completed abroad)  
, C-576/20, EU:C:2022:525, paragraph 35 and the case-law cited).  
44      For those purposes, the Court may extract from all the information provided by the national court, in particular from the grounds of the order for reference, the points of EU law which require interpretation in view of the subject matter of the dispute in the main proceedings (see, to that effect, judgment of 2 June 2022,   
HK/Danmark and HK/Privat  
, C-587/20, EU:C:2022:419, paragraph 18 and the case-law cited).  
45      In the present case, it is clear from the order for reference that the dispute in the main proceedings essentially concerns the question whether the competent personal data protection authorities may limit or prohibit the processing of such data as regards the possibility of filming the electoral process and, in particular, the vote count.  
46      Accordingly, it is to be understood that, by its third to sixth questions, which it is necessary to examine together, the referring court asks, in essence, whether Article 6(1)(e) and Article 58 of the GDPR must be interpreted as precluding the competent authorities of a Member State from adopting an administrative measure of general application which provides for the limitation or, where appropriate, the prohibition of video recording during the vote count at polling stations in elections in that Member State.  
47      In the first place, it should be pointed out that Article 6 of the GDPR sets out the conditions for the lawfulness of the processing of personal data.  
48      With regard more specifically to Article 6(1)(e) of the GDPR, which is specifically referred to in the request for a preliminary ruling, it follows from that provision that the processing of personal data is lawful if it is necessary for the performance of a task carried out in the public interest or a task carried out in the exercise of official authority vested in the controller.  
49      Article 6(1)(e) of the GDPR must be read in conjunction with Article 6(3) thereof, which states that the basis for the processing referred to in Article 6(1)(e) is to be laid down by EU law or by Member State law to which the controller is subject.  
50      The combined provisions of Article 6(1)(e) and Article 6(3) of the GDPR therefore allow Member States to adopt rules on the basis of which controllers may process personal data in the performance of a task carried out in the public interest or a task carried out in the exercise of official authority.  
51      In the present case, the referring court appears to consider, in the context of its fifth question, that some of the participants present at polling stations during the vote count could be performing a task carried out in the public interest within the meaning of Article 6(1)(e) of the GDPR.  
52      In that regard, it should be pointed out that the lawful processing of personal data by such participants on the basis of Article 6(1)(e) of the GDPR presupposes not only that they can be regarded as performing a task carried out in the public interest, but also that the processing of personal data for the purpose of performing such a task is founded on a legal basis referred to in Article 6(3) of that regulation.  
53      As the Commission rightly pointed out in its written observations, the guidelines at issue, adopted by the competent Bulgarian supervisory authorities, do not appear to constitute such a legal basis. On the contrary, they appear to constitute a measure aimed at protecting the personal data of the persons present at polling stations by limiting, in the case of media representatives, and prohibiting, in the case of other participants present at polling stations, the processing of such data by means of video recording during a specific phase of the electoral process, namely during the vote count.  
54      In the second place, it must be borne in mind that the powers of supervisory authorities are laid down in Article 58 of the GDPR.  
55      It follows from Article 58(2)(f) of the GDPR, read in the light of recital 129 of that regulation, that supervisory authorities are to have, inter alia, the power to impose a temporary or definitive limitation on the processing of personal data, including a ban, and that that power is to be exercised in accordance with the principle of proportionality. Similarly, in accordance with Article 58(3)(b) of the GDPR, each supervisory authority is to have the power to issue, on its own initiative or on request, opinions, in accordance with the law of the Member State concerned, to institutions and bodies other than the national parliament or the government of that Member State as well as to the public, on any issue related to the protection of personal data. Finally, in accordance with Article 58(4) of that regulation, the exercise of those powers is to be subject to appropriate safeguards, including effective judicial remedy.  
56      The description of Bulgarian law and of the guidelines at issue, as set out in the documents before the Court, does not make it possible to establish, subject to the matters to be verified by the referring court, that the competent Bulgarian authorities exceeded the powers available to them under Article 58(2)(f) and (3)(b) of the GDPR and, in particular, that the guidelines at issue do not comply with the principle of proportionality.  
57      In that regard, the referring court notes that the guidelines at issue limit, in the case of media representatives, and prohibit, in the case of other participants present at polling stations, the processing of personal data by means of video recording during a specific phase of the electoral process, namely during the opening of ballot boxes and the determination of the election results. By contrast, those guidelines do not appear to limit the ability of participants present at polling stations during the vote count to observe the opening of the ballot boxes and the determination of the election results, thus ensuring the transparency, objectivity and legitimacy of the electoral process, the equal treatment of the participants in the process and the freedom of expression and the right to information, in accordance with the objective of those guidelines.  
58      Accordingly, it must be held that the guidelines at issue are intended, in accordance with the principle of data minimisation referred to in Article 5(1)(c) of the GDPR, to minimise the interference with the right to the protection of personal data caused by video recording the electoral process.  
59      In the third and last place, it must be borne in mind, so far as is relevant, that Member States may provide for exemptions and derogations from certain provisions of the GDPR in order to reconcile the right to the protection of personal data with the freedom of expression and information.  
60      Under Article 85(1) of the GDPR, Member States are by law to reconcile the right to the protection of personal data pursuant to that regulation with the right to freedom of expression and information, including the processing of personal data for journalistic purposes. According to Article 85(2) of that regulation, Member States are to provide for exemptions or derogations from certain chapters of the GDPR, including Chapter II, which contains Article 6 of the GDPR. Those exemptions or derogations must be limited to what is necessary to reconcile the right to the protection of personal data with the freedom of expression and information.  
61      In the light of the foregoing considerations, the answer to the third to sixth questions is that Article 6(1)(e) and Article 58 of the GDPR must be interpreted as not precluding the competent authorities of a Member State from adopting an administrative measure of general application which provides for the limitation or, where appropriate, the prohibition of video recording during the vote count at polling stations in elections in that Member State.  
   
Costs  
62      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Eighth Chamber) hereby rules:  
1.        
Article 2(2)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
must be interpreted as meaning that the processing of personal data in the context of the organisation of elections in a Member State is not excluded from the scope of that regulation.  
2.        
Article 6(1)(e) and Article 58 of Regulation 2016/679  
must be interpreted as meaning that those provisions do not preclude the competent authorities of a Member State from adopting an administrative measure of general application which provides for the limitation or, where appropriate, the prohibition of video recording during the vote count at polling stations in elections in that Member State.

ID: 4cc9b1f3-d012-44fe-8e69-7ca7d2ff20cd

of 16 Nov 2023, C-333/22 (  
Ligue des droits humains  
)  
Law Enforcement Directive   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
   
JUDGMENT OF THE COURT (Fifth Chamber)  
16 November 2023 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Directive (EU) 2016/680 – Article 17 – Exercise of the rights of the data subject through the supervisory authority – Verification of the lawfulness of the data processing – Article 17(3) – Obligation to provide the data subject with a minimum of information – Scope – Validity – Article 53 – Right to seek an effective judicial remedy against the supervisory authority – Concept of a ‘legally binding decision’ – Charter of Fundamental Rights of the European Union – Article 8(3) – Control by an independent authority – Article 47 – Right to effective judicial protection)  
In Case C-333/22,  
REQUEST for a preliminary ruling under Article 267 TFEU from the cour d’appel de Bruxelles (Court of Appeal, Brussels, Belgium), made by decision of 9 May 2022, received at the Court on 20 May 2022, in the proceedings  
Ligue des droits humains ASBL,  
BA  
v  
Organe de contrôle de l’information policière,  
THE COURT (Fifth Chamber),  
composed of E. Regan, President of the Chamber, Z. Csehi, M. Ilešič, I. Jarukaitis and D. Gratsias (Rapporteur), Judges,  
Advocate General: L. Medina,  
Registrar: M. Siekierzyńska, Administrator,  
having regard to the written procedure and further to the hearing on 29 March 2023,  
after considering the observations submitted on behalf of:   
–        Ligue des droits humains ASBL and BA, by C. Forget, avocate,  
–        the Organe de contrôle de l’information policière (OCIP), by J. Bosquet and J.-F. De Bock, advocaten,  
–        the Belgian Government, by P. Cottin, J.-C. Halleux, C. Pochet and A. Van Baelen, acting as Agents, and by N. Cariat, C. Fischer, B. Lombaert and J. Simba, avocats,  
–        the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
–        the French Government, by J. Illouz, acting as Agent,  
–        the European Parliament, by S. Alonso de León, O. Hrstková Šolcová, P. López-Carceller and M. Thibault, acting as Agents,  
–        the European Commission, by A. Bouchagiar, H. Kranenborg, A.-C. Simon and F. Wilman, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 15 June 2023,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns, first, the interpretation of Article 8(3) and Article 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’) and, secondly, the validity, in the light of the abovementioned provisions of the Charter, of Article 17 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).  
2        The request has been made in proceedings between Ligue des droits humains ASBL and BA, on the one hand, and, on the other, the Organe de contrôle de l’information policière (OCIP) (Supervisory Body for Police Information (OCIP), Belgium) regarding the exercise, through that body, of BA’s rights relating to the personal data concerning him, processed by the Belgian police service and on the basis of which the Autorité nationale de sécurité (National Security Authority, Belgium) rejected a request for security clearance made by BA.  
   
Legal context  
   
European Union law  
3        Recitals 7, 10, 43, 46, 48, 75, 82, 85 and 86 of Directive 2016/680 state:  
‘(7)      Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that end, the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should be equivalent in all Member States. Effective protection of personal data throughout the [European] Union requires the strengthening of the rights of data subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.  
…  
(10)      In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.  
…  
(43)      A natural person should have the right of access to data which [have] been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. …  
…  
(46)      Any restriction of the rights of the data subject must comply with the Charter and with the [Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950], as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.  
…  
(48)      Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. …  
…  
(75)      The establishment in Member States of supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and should contribute to their consistent application throughout the Union in order to protect natural persons with regard to the processing of their personal data. …  
…  
(82)      In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the TFEU as interpreted by the Court of Justice, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective, and advisory powers which constitute necessary means to perform their tasks. …  
…  
(85)      Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. …  
(86)      Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, that right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.’  
4        Article 1 of that directive, headed ‘Subject matter and objectives’, provides, in paragraphs 1 and 2 thereof:  
‘1.      This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.  
2.      In accordance with this Directive, Member States shall:  
(a)      protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and  
(b)      ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.’  
5        That directive contains a Chapter III, entitled ‘Rights of the data subject’, which includes, inter alia, Articles 13 to 17 of the directive. Article 13 thereof, entitled ‘Information to be made available or given to the data subject’, sets out, in paragraph 1 thereof, the obligation for the Member States to provide that the controller must make available to the data subject a minimum degree of information, such as, inter alia, the identity and contact details of the controller. In addition, it lists, in paragraph 2 thereof, the additional information that the Member States must, by law, require the controller to provide to the data subject in order to enable the exercise of his or her rights. In paragraphs 3 and 4 thereof, it states:  
‘3.      Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:  
(a)      avoid obstructing official or legal inquiries, investigations or procedures;  
(b)      avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;  
(c)      protect public security;  
(d)      protect national security;  
(e)      protect the rights and freedoms of others.  
4.      Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.’  
6        Article 14 of that directive, headed ‘Right of access by the data subject’, is worded as follows:  
‘Subject to Article 15, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data …’  
7        Under Article 15 of Directive 2016/680, entitled ‘Limitations to the right of access’:  
‘1.      Member States may adopt legislative measures restricting, wholly or partly, the data subject’s right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:  
(a)      avoid obstructing official or legal inquiries, investigations or procedures;  
(b)      avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;  
(c)      protect public security;  
(d)      protect national security;  
(e)      protect the rights and freedoms of others.  
2.      Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under points (a) to (e) of paragraph 1.  
3.      In the cases referred to in paragraphs 1 and 2, Member States shall provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.  
4.      Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.’  
8        Article 16 of that directive, entitled ‘Right to rectification or erasure of personal data and restriction of processing’, provides:  
‘1.      Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purposes of the processing, Member States shall provide for the data subject to have the right to have incomplete personal data completed, …  
2.      Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.  
3.      Instead of erasure, the controller shall restrict processing where:  
(a)      the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or  
(b)      the personal data must be maintained for the purposes of evidence.  
…  
4.      Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:  
(a)      avoid obstructing official or legal inquiries, investigations or procedures;  
(b)      avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;  
(c)      protect public security;  
(d)      protect national security;  
(e)      protect the rights and freedoms of others.  
Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.  
…’  
9        Article 17 of that directive, entitled ‘Exercise of rights by the data subject and verification by the supervisory authority’, provides:  
‘1.      In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.  
2.      Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1.  
3.      Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.’  
10      Article 42 of that directive, entitled ‘Independence’, provides, in paragraph 1 thereof:  
‘Each Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.’  
11      Article 46 of Directive 2016/680, entitled ‘Tasks’, provides, in paragraph 1 thereof:  
‘Each Member State shall provide, on its territory, for each supervisory authority to:  
(a)      monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;  
…  
(f)      deal with complaints lodged by a data subject, … and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, …  
(g)      check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;  
…’  
12      Under Article 47 of that directive, entitled ‘Powers’:  
‘1.      Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.  
2.      Each Member State shall provide by law for each supervisory authority to have effective corrective powers such as, for example:  
(a)      to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions adopted pursuant to this Directive;  
(b)      to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 16;  
(c)      to impose a temporary or definitive limitation, including a ban, on processing.  
…  
4.      The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, as set out in Union and Member State law in accordance with the Charter.  
…’  
13      Article 52 of that directive, entitled ‘Right to lodge a complaint with a supervisory authority’, provides, in paragraph 1 thereof:  
‘Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.’  
14      Article 53 of that directive, entitled ‘Right to an effective judicial remedy against a supervisory authority’, states, in paragraph 1 thereof:  
‘Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.’  
15      Article 54 of Directive 2016/680, entitled ‘Right to an effective judicial remedy against a controller or processor’, is worded as follows:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.’  
   
Belgian law  
16      The loi relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel (Law on the protection of natural persons with regard to the processing of personal data) of 30 July 2018 (  
Moniteur belge  
, 5 September 2018, p. 68616) (‘the LPD’) transposes, in Title 2 thereof, Directive 2016/680. The rights set out in Articles 13 to 16 of that directive are provided for in Chapter III of that title, specifically in Articles 37 to 39 of that law.  
17      Article 42 of the LPD provides:  
‘Any request to exercise the rights set out in this chapter with respect to the police services … or to the Inspection générale de la police fédérale et de la police locale [(General Inspectorate of the Federal and Local Police, Belgium)] shall be made to the supervisory authority referred to in Article 71.  
In the cases referred to in Articles 37(2), 38(2) [and] 39(4) …, the supervisory authority referred to in Article 71 shall inform the data subject only that the necessary verifications have been carried out.  
Notwithstanding paragraph 2, the supervisory authority referred to in Article 71 may communicate certain contextual information to the data subject.  
The King shall determine, following opinion from the supervisory authority referred to in Article 71, the category of contextual information that may be communicated to the data subject by that authority.’  
18      According to the cour d’appel de Bruxelles (Court of Appeal, Brussels, Belgium), the referring court, no Royal Decree has been adopted in order to implement the fourth paragraph of Article 42 of the LPD.  
19      Under Article 71(1) of the LPD:  
An independent supervisory authority for police information is hereby created at the Chamber of Representatives, under the name [Supervisory Body for Police Information].  
…  
[It shall be] responsible for:  
1.      supervising the application of this Title …  
2.      monitoring the processing of the information and personal data covered by Articles 44/1 to 44/11/13 of the loi du 5 août 1992 sur la fonction de police (Law of 5 August 1992 on the police service), including that held in the data banks referred to in Article 44/2 of that law;  
3.      any other task organised by or under other laws.’  
20      Chapter I of Title 5 of the LPD is entitled ‘Action for an injunction’. Article 209, which is contained in that chapter, reads as follows:  
‘Without prejudice to any other judicial, administrative or extra-judicial remedy, the president of the court of first instance, sitting as if hearing interim proceedings, may determine that processing has been carried out which constitutes a breach of the statutory or regulatory provisions on the protection of natural persons with regard to the processing of their personal data, and grant an injunction prohibiting such processing.  
The president of the court of first instance, sitting as if hearing interim proceedings, shall hear any application relating to the right granted by or by virtue of the law to obtain access to personal data, as well as any application seeking rectification, erasure or prevention of the use of any personal data which are inaccurate or, having regard to the purpose of the processing, incomplete or irrelevant, or of which the recording, disclosure or storage is prohibited, to the processing of which the data subject has objected or which have been retained for longer than is permitted.’  
21      Article 240(4) of the LPD provides that:  
‘[The OCIP]  
…  
4.      shall deal with complaints, investigate the subject matter of the complaint so far as necessary, and inform the complainant of the progress and the outcome of the investigation within a reasonable time, particularly where further investigation or cooperation with another supervisory authority is necessary. …’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
22      In 2016, BA, who at that time was employed on a part-time basis with a charity, sought security clearance from the National Security Authority in order to participate in the assembly and disassembly of the installations for the tenth ‘European Development Days’ event in Brussels (Belgium).  
23      By letter of 22 June 2016, that authority refused BA security clearance, on the ground that it was apparent from the personal data which had been made available to it that that person had participated in 10 demonstrations between 2007 and 2016 and that such factors prevented him from being granted such clearance under the rules applicable, inter alia for reasons of State security and preservation of the constitutional democratic order. No appeal was brought against that decision.  
24      On 4 February 2020, BA’s legal adviser requested the OCIP to identify the controllers responsible for processing the personal data at issue and to order them to provide his client with access to all the information concerning him in order to enable him to exercise his rights within an appropriate period.  
25      By email of 6 February 2020, the OCIP acknowledged receipt of that request. It indicated that BA only had an indirect right of access to those data, while also stating that it was itself going to verify the lawfulness of any data processing in the Banque de données nationale générale (General National Data Bank), namely the database used by all the national police services. It also stated that it had the power to order the police to erase or amend data, if necessary, and that once the checks had been completed, it would inform BA that the necessary verifications have been carried out.  
26      By email of 22 June 2020, the OCIP stated as follows to BA’s legal adviser:  
‘…  
I inform you, in accordance with Article 42 of [the LPD], that the [OCIP] has carried out the necessary verifications.  
This means that your client’s personal data have been checked against the police data banks with a view to ensuring the lawfulness of any processing.  
If necessary, the personal data have been amended or erased.  
As I informed you in my email of 2 June, Article 42 of the LPD does not permit the [OCIP] to provide any further information.’  
27      On 2 September 2020, Ligue des droits humains and BA, on the basis of the second paragraph of Article 209 of the LPD, submitted an application for interim relief before the tribunal de première instance francophone de Bruxelles (Brussels Court of First Instance (French-speaking), Belgium).  
28      In the first place, the applicants in the main proceedings requested that court to declare the application for interim relief admissible, and, in the alternative, to refer a question to the Court of Justice on whether, in essence, Article 47(4) of Directive 2016/680, read in the light of recitals 85 and 86 of that directive and in conjunction with Article 8(3) and Article 47 of the Charter, precluded Articles 42 and 71 of the LPD, inasmuch as those provisions did not provide for any judicial remedy against decisions taken by the OCIP.  
29      In the second place, as to the substance, they requested access to all personal data concerning BA, through the OCIP, and the identification, by the latter, of the controllers and any recipients of those data.  
30      In the event that the court seised were to hold that Article 42(2) of the LPD allowed access to the personal data processed by the police services to be systematically restricted, they requested, in the alternative, that a question be referred to the Court of Justice concerning, in essence, whether Articles 14, 15 and 17 of Directive 2016/680, read in conjunction with Articles 8 and 47 and Article 52(1) of the Charter, were to be interpreted as precluding national legislation allowing a general and systematic derogation from the right of access to personal data where, first, that right was exercised through the supervisory authority and, secondly, that authority could merely state to the data subject that it had carried out all the necessary verifications without informing him or her of the personal data being processed and of the recipients, irrespective of the intended purpose.  
31      By order of 17 May 2021, the tribunal de première instance francophone de Bruxelles (Brussels Court of First Instance (French-speaking)) declared that it had ‘no jurisdiction’ to hear and determine that application for interim relief.  
32      On 15 June 2021, the applicants in the main proceedings brought an appeal against that order before the cour d’appel de Bruxelles (Court of Appeal, Brussels), the referring court. In essence, they reiterated the requests they had made at first instance.  
33      In that context, the referring court observes, inter alia, in essence that, in the event that a person does not have the right to exercise in person the rights provided for by Directive 2016/680, the action for an injunction provided for in Article 209 et seq. of the LPD cannot be put into effect. First, such an action can be brought against the controller, but not against the supervisory authority itself. Secondly, nor can it be exercised by that person, in the present case, BA, against the controller, since the exercise of that person’s rights is entrusted to that authority. Lastly, the very succinct information provided by the OCIP to BA does not enable either BA or a court to determine whether that supervisory authority has exercised BA’s rights correctly. It adds that, although the LPD provides that that action for an injunction is without prejudice to any other judicial, administrative or extra-judicial remedy, any other such remedy sought by BA would encounter the same problems.  
34      In those circumstances, the cour d’appel de Bruxelles (Court of Appeal, Brussels) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Do Articles 47 and 8(3) of [the Charter] require provision to be made for a judicial remedy against an independent supervisory authority such as the [OCIP] where it exercises the rights of the data subject vis-à-vis the controller?  
(2)      Does Article 17 of Directive 2016/680 comply with Articles 47 and 8(3) of [the Charter], as interpreted by the Court of Justice, in that it obliges the supervisory authority – which exercises the rights of the data subject vis-à-vis the controller – only to inform the data subject “that all necessary verifications or a review by the supervisory authority have taken place” and “of his or her right to seek a judicial remedy”, when such information does not enable any   
a posteriori  
 review to be conducted as regards the action taken and assessment made by the supervisory authority in the light of the data of the data subject and the obligations of the controller?’  
   
Consideration of the questions referred  
   
The first question  
35      As a preliminary point, it is apparent from the request for a preliminary ruling that the questions of the referring court concern the existence, on the basis of Article 53(1) of Directive 2016/680, read in the light of Article 47 of the Charter, of an obligation for the Member States to provide for a right to an effective judicial remedy against the competent national supervisory authority, when a provision of national law is implemented which transposes Article 17 of that directive, according to which, in the cases covered by Article 13(3), Article 15(3) and Article 16(4) of that directive, the rights of the data subject may be exercised through such a supervisory authority.  
36      In addition, it must be observed that the answer to that question is dependent on the nature and scope of the task and powers of the supervisory authority in connection with the exercise of the data subject’s rights, provided for in Article 17 of Directive 2016/680. That task and those powers are set out in Article 46(1)(g) and Article 47(1) and (2) of that directive and must be analysed in the light of Article 8(3) of the Charter, which requires that compliance with the rules on the protection of personal data, set out in paragraphs 1 and 2 of Article 8 thereof, is to be subject to control by an independent authority.  
37      Therefore, the referring court must be understood as asking, in essence, by its first question, whether Article 17 of Directive 2016/680, read in conjunction with Article 46(1)(g), Article 47(1) and (2) and Article 53(1) of that directive, and with Article 8(3) and Article 47 of the Charter, must be interpreted as meaning that, where the rights of a data subject have been exercised, pursuant to Article 17 of that directive, through the competent supervisory authority, that data subject must have available to him or her an effective judicial remedy against that authority.  
38      It must be recalled at the outset that, under Article 53(1) of Directive 2016/680, Member States must provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.  
39      It must therefore be determined whether a supervisory authority adopts such a decision where, pursuant to Article 17 of that directive, the rights of the data subject set out by that directive are exercised through that supervisory authority.  
40      In this connection, under Article 17(1) of Directive 2016/680, ‘in the cases referred to in Article 13(3), Article 15(3) and Article 16(4)’ of that directive, Member States are under an obligation to adopt measures ‘providing that the rights of the data subject may also be exercised through the competent supervisory authority’.  
41      As indicated by the use of the adverb ‘also’ and as the Advocate General in essence observed in points 41 and 42 of her Opinion, the indirect exercise of the rights of the data subject through the competent supervisory authority, provided for in that provision, is an additional guarantee offered to that data subject that his or her personal data are processed lawfully, where national legislative provisions limit the direct exercise before the controller of the right to receive further information, referred to in Article 13(2) of Directive 2016/680, the right of access to those data, set out in Article 14 of that directive, or of the right to obtain their rectification, erasure or a restriction of processing under the conditions of Article 16(1) to (3) of that directive.  
42      Having regard to the specific nature of the purposes for which the data processing covered by that directive is carried out, to which attention is drawn, in particular, in recital 10 thereof, Article 13(3) and Article 15(1) of Directive 2016/680 authorise the national legislature to limit the direct exercise, on the one hand, of the right to information, and, on the other hand, of the right of access, ‘to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person’, in order to ‘avoid obstructing official or legal inquiries, investigations or procedures’, ‘avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties’, ‘protect public security’, ‘protect national security’ or ‘protect the rights and freedoms of others’. In addition, Article 15(3) of that directive provides that the controller may omit to inform the data subject of any refusal or restriction of access and of the reasons for the refusal or the restriction where the provision of that information would undermine one of the abovementioned public interest purposes.  
43      Likewise, Article 16(4) of that directive authorises the national legislature to restrict the obligation on the controller to ‘inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal’ for the same public interest purposes, ‘to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned’.  
44      Therefore, in that context, as is apparent from recital 48 of that directive, the indirect exercise of the rights referred to in paragraph 41 above through the competent supervisory authority must be regarded as necessary for the protection of those rights, their direct exercise before the controller being difficult or even impossible.  
45      To that end, Article 46(1)(g) of Directive 2016/680 requires that each competent national authority must be entrusted with the task of checking the lawfulness of processing pursuant to Article 17 of that directive, that is to say following a request made on the basis of the latter provision.  
46      Moreover, it is apparent, inter alia, from Article 47(1) and (2) of that directive that each supervisory authority must have, under the national legislation, not only ‘effective investigative powers’ but also ‘effective corrective powers’.  
47      Those provisions must be read in the light of the requirement stated in Article 8(3) of the Charter, that compliance with the rules on the right of everyone to the protection of personal data, set out in paragraphs 1 and 2 of that article, must be ‘subject to control by an independent authority’, and, in particular, the requirement set out in the second sentence of paragraph 2 thereof, that ‘everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified’. As is confirmed by settled case-law, the establishment of an independent supervisory authority is intended to ensure the effectiveness and reliability of the monitoring of compliance with the rules concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim (see, to that effect, Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, paragraph 229 and the case-law cited).  
48      Thus, where such a supervisory authority acts in order to ensure the exercise of the rights of the data subject on the basis of Article 17 of Directive 2016/680, its task falls entirely within the definition, in EU primary law, of its role, since that definition entails, inter alia, the monitoring of compliance with the data subject’s rights of access and of rectification. It follows that, in accomplishing that specific task, as with any other task, the supervisory authority must be able to exercise the powers which are conferred on it under Article 47 of that directive by acting with complete independence, in accordance with the Charter and as stated in recital 75 of that directive.  
49      In addition, at the end of the verification of the lawfulness of processing, the competent supervisory authority must, under the first sentence of Article 17(3) of that directive, inform the data subject ‘at least that all necessary verifications or a review by the supervisory authority have taken place’.  
50      As observed, in essence, by the Advocate General in point 65 of her Opinion, it must be inferred from all those provisions that, when the competent supervisory authority informs the data subject of the result of the verifications made, it brings to his or her knowledge the decision it has made in his or her regard to close the verification process, that decision necessarily affecting the legal position of the data subject. That decision therefore constitutes a ‘legally binding decision’ with regard to the data subject, within the meaning of Article 53(1) of Directive 2016/680, irrespective of whether and to what extent that authority has found the processing of the data concerning that subject to be lawful or adopted corrective measures.  
51      Indeed, recital 86 of that directive states that the concept of ‘legally binding decision’ within the meaning of that directive must be understood as referring to a decision which produces legal effects concerning the data subject, in particular, a decision concerning the exercise of investigative, corrective and authorisation powers by the supervisory authority or concerning the dismissal or rejection of complaints.  
52      Therefore, the data subject must be able to obtain judicial review of the merits of such a decision on the basis of Article 53(1) of Directive 2016/680, and, in particular, of the manner in which the supervisory authority performed its obligation, resulting from Article 17 of that directive and to which Article 46(1)(g) of that directive refers, to carry out ‘all necessary verifications’ and, as the case may be, exercised its corrective powers.  
53      That conclusion is, moreover, borne out by recital 85 of Directive 2016/680, from which it is apparent that any data subject should have the right to an effective judicial remedy against a supervisory authority where that authority ‘does not act where such action is necessary to protect the rights of the data subject’.  
54      Lastly, such an interpretation is in accordance with Article 47 of the Charter, since, as is apparent from settled case-law, that right must be must be accorded to any person relying on rights or freedoms guaranteed by EU law against a decision adversely affecting him or her which is such as to undermine those rights or freedoms (see, to that effect, judgment of 26 January 2023,   
Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)  
, C-205/21, EU:C:2023:49, paragraph 87 and the case-law cited).  
55      Having regard to all the foregoing considerations, the answer to the first question is that Article 17 of Directive 2016/680, read in conjunction with Article 46(1)(g), Article 47(1) and (2) and Article 53(1) of that directive, and with Article 8(3) and Article 47 of the Charter, must be interpreted as meaning that where the rights of a data subject have been exercised, pursuant to Article 17 of that directive, through the competent supervisory authority and that authority informs that data subject of the result of the verifications carried out, that data subject must have an effective judicial remedy against the decision of that authority to close the verification process.  
   
The second question  
56      By its second question, the referring court asks, in essence, whether Article 17(3) of Directive 2016/680 is valid having regard to Article 8(3) and Article 47 of the Charter in so far as it obliges the supervisory authority only to inform the data subject (i) that all necessary verifications or a review by the supervisory authority have taken place and (ii) that that person has a right to seek a judicial remedy, since such information does not allow any judicial review of the action taken and the assessment made by the supervisory authority, in the light of the data processed and of the obligations of the controller.  
57      First, it should be noted in this respect that, in accordance with a general principle of interpretation, an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Thus, if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law (judgment of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraph 86 and the case-law cited).  
58      Secondly, the right to an effective judicial remedy, guaranteed in Article 47 of the Charter, requires, in principle, that the person concerned must be able to ascertain the reasons on which the decision taken in relation to him or her is based, so as to make it possible for him or her to defend his or her rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in his or her applying to the court with jurisdiction, and in order to put the latter fully in a position in which it may carry out the review of the lawfulness of that decision (see, to that effect, judgment of 4 June 2013,   
ZZ  
, C-300/11, EU:C:2013:363, paragraph 53 and the case-law cited).  
59      Although that right is not an absolute right and, in accordance with Article 52(1) of the Charter, limitations may be placed upon it, that is on condition that those limitations are provided for by law, they respect the essence of the rights and freedoms at issue and, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 26 January 2023,   
Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)  
, C-205/21, EU:C:2023:49, paragraph 89 and the case-law cited).  
60      In the present case, it must be observed that, so far as concerns the decision of the competent supervisory authority identified in paragraph 50 above, Article 17(3) of Directive 2016/680 establishes, with respect to that supervisory authority, an obligation to provide a minimum of information, providing that it is to inform the data subject ‘at least that all necessary verifications or a review by the supervisory authority have taken place’ and of ‘his or her right to seek a judicial remedy’.  
61      It follows that, since that provision does not preclude, in certain situations, in accordance with the rules adopted by the national legislature to implement it, the supervisory authority from being able, or even obliged, to confine itself to providing the minimum information referred to in the preceding paragraph, without any other details, in particular where those rules seek to avoid compromising the public interest purposes provided for in Article 13(3), Article 15(1) and Article 16(4) of that directive, as set out in paragraphs 42 and 43 above, it is liable to give rise to a limitation on the right to an effective judicial remedy, guaranteed in Article 47 of the Charter.  
62      That said, in the first place, it must be noted that such a limitation is expressly provided for by Directive 2016/680 and that it therefore complies with the condition laid down in Article 52(1) of the Charter, according to which any limitation on the exercise of a fundamental right must be ‘provided for by law’.  
63      In the second place, the fact that Article 17(3) of Directive 2016/680 allows Member States to restrict, in certain cases, the statement of reasons for that decision to the minimum particulars set out in that provision, does not mean, as the Advocate General in essence states in point 89 of her Opinion, that it is possible in all circumstances to reduce the information provided to the data subject to solely those particulars.  
64      That provision must be interpreted in the light of Article 52(1) of the Charter, so that the other criteria set out in that latter provision must be satisfied. That means holding that Article 17(3) of that directive requires Member States to ensure that the provisions of national law implementing it, first, respect the essence of the data subject’s right to effective judicial protection and, secondly, are based on a weighing up of the public interest purposes warranting limitation of that information and of the fundamental rights and legitimate interests of that data subject, in accordance with the principles of necessity and of proportionality, like the weighing up which must be carried out by the national legislature when it implements the limitations provided for in Article 13(3), Article 15(3) and Article 16(4) of that directive.  
65      In particular, where (i) it is required by the protection of the right of the data subject to an effective judicial remedy against the decision to close the verification process and (ii) it is not precluded by the public interest purposes referred to in Article 13(3), Article 15(3) and Article 16(4) of Directive 2016/680, the onus is on the Member States to provide that the information disclosed to the data subject may go beyond the minimum information provided for by Article 17(3) of that directive, so as to make it possible for him or her to defend his or her rights and to decide, with full knowledge of the facts, whether there is any point in him or her applying to the court with jurisdiction.  
66      Likewise, the national measures implementing that latter provision must, to the extent possible, leave a degree of discretion to the competent supervisory authority, in accordance with the independence characterising such an authority under Article 8(3) of the Charter, to determine whether the framework established by the national legislation in line with the requirements noted in paragraph 65 above precludes it from communicating to that data subject, at least in brief, the result of its verifications and any corrective measures which it has taken. In this connection, as the Advocate General observed, in essence, in points 73 and 74 of her Opinion, it is for that authority, in compliance with that national legislative framework, to engage in a confidential dialogue with the controller and, at the end of that dialogue, to decide on which information is necessary for the data subject to exercise his or her right to an effective judicial remedy and may be communicated to him or her without compromising the public interest purposes referred to in paragraph 65 above.  
67      Moreover, should that framework require that the information provided by the supervisory authority be limited to that provided for in Article 17(3) of Directive 2016/680, it is nevertheless for the Member States, in the exercise of their procedural autonomy, to implement the measures necessary to guarantee, in accordance with Article 53(1) of that directive, an effective judicial review both of the existence and of the merits of the reasons which warranted the limitation on that information and of the correct execution, by the supervisory authority, of its task of verifying the lawfulness of the processing. In that regard, the concept of ‘effective judicial remedy’ referred to in the latter provision must be read in the light of recital 86 of that directive, under which the courts before which actions against a supervisory authority are brought ‘should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it’.  
68      In particular, Member States must ensure that the court with jurisdiction has at its disposal and applies techniques and rules of procedural law which accommodate, on the one hand, legitimate considerations in relation to the public interest purposes referred to in Article 13(3), Article 15(3) and Article 16(4) of Directive 2016/680, those purposes having been taken into consideration by the national legislation to limit the information provided to the data subject and, on the other hand, the need to ensure sufficient compliance with the data subject’s procedural rights, such as the right to be heard and the adversarial principle (see, to that effect, judgment of 4 June 2013,   
ZZ  
, C-300/11, EU:C:2013:363, paragraph 57 and the case-law cited).  
69      In the context of the judicial review of the correct application of Article 17 of that directive by the supervisory authority, it is incumbent upon the Member States to lay down rules enabling the court with jurisdiction to examine both all the grounds and the related evidence on the basis of which that authority based, within that framework, the verification of the lawfulness of the processing of the data at issue as well as the conclusions which it drew from that verification (see, to that effect, judgment of 4 June 2013,   
ZZ  
, C-300/11, EU:C:2013:363, paragraph 59 and the case-law cited).  
70      In that regard, as the European Parliament noted in its observations, Article 15(4) of Directive 2016/680 provides that the controller must document the factual or legal reasons on which it has based the decision by which it limited, wholly or partly, the rights of access of the data subject and that that information must be made available to the supervisory authorities. As that institution suggested, that provision, read in conjunction with Articles 17 and 53 of that directive and in the light of Article 47 of the Charter, as interpreted by the case-law recalled in paragraphs 68 and 69 above, implies that that information must also be made available to the court before which an action against the supervisory authority has been brought, seeking review of the correct application of Article 17 of that directive.  
71      Thus, it is apparent from paragraphs 63 to 70 above that the limitation provided for in Article 17 of Directive 2016/680 respects the essence of the data subject’s right to an effective judicial remedy against the supervisory authority’s decision to close the procedure provided for in that provision and the principles of necessity and proportionality, in accordance with Article 52(1) of the Charter.  
72      Having regard to all the foregoing considerations, it must be concluded that the examination of the second question has revealed nothing capable of affecting the validity of Article 17(3) of Directive 2016/680.  
   
Costs  
73      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Fifth Chamber) hereby rules:  
1.        
Article 17 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, read in conjunction with Article 46(1)(g), Article 47(1) and (2) and Article 53(1) of that directive and with Article 8(3) and Article 47 of the Charter of Fundamental Rights of the European Union,  
must be interpreted as meaning that where the rights of a data subject have been exercised, pursuant to Article 17 of that directive, through the competent supervisory authority and that authority informs that data subject of the result of the verifications carried out, that data subject must have an effective judicial remedy against the decision of that authority to close the verification process.  
2.        
The examination of the second question has revealed nothing capable of affecting the validity of Article 17(3) of Directive 2016/680.

ID: 4fe58eba-6f13-45d1-85e1-0611962f95f0

of 7 Dec 2023, C-26/22 (  
SCHUFA Holding  
)  
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Right to an effective remedy against a supervisory authority   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness, fairness and transparency   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to object   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
   
JUDGMENT OF THE COURT (First Chamber)  
7 December 2023 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 5(1)(a) – Principle of ‘lawfulness’ – Point (f) of the first subparagraph of Article 6(1) – Necessity of processing for the purposes of the legitimate interests pursued by the controller or by a third party – Article 17(1)(d) – Right to erasure where personal data have been unlawfully processed – Article 40 – Codes of conduct – Article 78(1) – Right to an effective judicial remedy against a supervisory authority – Decision taken by the supervisory authority on a complaint – Scope of judicial review of that decision – Credit information agencies – Storage of data from a public register relating to the discharge of remaining debts in favour of a person – Storage period)  
In Joined Cases C-26/22 and C-64/22,  
REQUESTS for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), made by decisions of 23 December 2021 and 31 January 2022, received at the Court on 11 January 2022 and 2 February 2022, in the proceedings  
UF  
 (C-26/22),  
AB  
 (C-64/22)  
v  
Land Hessen,  
intervener:  
SCHUFA Holding AG,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, T. von Danwitz, P.G. Xuereb, A. Kumin (Rapporteur) and I. Ziemele, Judges,  
Advocate General: P. Pikamäe,  
Registrar: K. Hötzel, Administrator,  
having regard to the written procedure and further to the hearing on 26 January 2023,  
after considering the observations submitted on behalf of:  
–        UF and AB, by R. Rohrmoser and S. Tintemann, Rechtsanwälte,  
–        the Land Hessen, by M. Kottmann and G. Ziegenhorn, Rechtsanwälte,  
–        SCHUFA Holding AG, by G. Thüsing and U. Wuermeling, Rechtsanwalt,  
–        the German Government, by J. Möller and P.-L. Krüger, acting as Agents,  
–        the Portuguese Government, by P. Barros da Costa, J. Ramos and C. Vieira Guerra, acting as Agents,  
–        the European Commission, by A. Bouchagiar, F. Erlbacher, H. Kranenborg and W. Wils, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 16 March 2023,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern the interpretation of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’) and of point (f) of the first subparagraph of Article 6(1), Article 17(1)(d), Article 40, Article 77(1) and Article 78(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2; ‘the GDPR’).  
2        The requests have been made in two sets of proceedings between UF (Case C-26/22) and AB (Case C-64/22), on the one hand, and the Land Hessen (Federal State of Hesse, Germany), on the other hand, concerning the refusal of the Hessischer Beauftragter für Datenschutz und Informationsfreiheit (Data Protection and Freedom of Information Commissioner for the Federal State of Hesse, Germany; ‘the HBDI’) to order SCHUFA Holding AG (‘SCHUFA’) to delete data held by it relating to the discharge from remaining debts in favour of UF and of AB.  
   
Legal context  
   
European Union law  
   
Directive 2008/48/EC  
3        According to recitals 26 and 28 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ 2008 L 133, p. 66):  
‘(26)      … In the expanding credit market, in particular, it is important that creditors should not engage in irresponsible lending or give out credit without prior assessment of creditworthiness, and the Member States should carry out the necessary supervision to avoid such behaviour and should determine the necessary means to sanction creditors in the event of their doing so. … [C]reditors should bear the responsibility of checking individually the creditworthiness of the consumer. …  
…  
(28)      To assess the credit status of a consumer, the creditor should also consult relevant databases; the legal and actual circumstances may require that such consultations vary in scope. To prevent any distortion of competition among creditors, it should be ensured that creditors have access to private or public databases concerning consumers in a Member State where they are not established under non-discriminatory conditions compared with creditors in that Member State.’  
4        Article 8(1) of that directive, that article being headed ‘Obligation to assess the creditworthiness of the consumer’, provides:  
‘Member States shall ensure that, before the conclusion of the credit agreement, the creditor assesses the consumer’s creditworthiness on the basis of sufficient information, where appropriate obtained from the consumer and, where necessary, on the basis of a consultation of the relevant database. Member States whose legislation requires creditors to assess the creditworthiness of consumers on the basis of a consultation of the relevant database may retain this requirement.’  
   
Directive 2014/17/EU  
5        According to recitals 55 and 59 of Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ 2014 L 60, p. 34):  
‘(55)      It is essential that the consumer’s ability and propensity to repay the credit is assessed and verified before a credit agreement is concluded. That assessment of creditworthiness should take into consideration all necessary and relevant factors that could influence a consumer’s ability to repay the credit over its lifetime. …  
…  
(59)      Consultation of a credit database is a useful element in the assessment of creditworthiness. …’  
6        Entitled ‘Obligation to assess the creditworthiness of the consumer’, Article 18 of that directive provides, in paragraph 1 thereof:  
‘Member States shall ensure that, before concluding a credit agreement, the creditor makes a thorough assessment of the consumer’s creditworthiness. That assessment shall take appropriate account of factors relevant to verifying the prospect of the consumer to meet his obligations under the credit agreement.’  
7        Entitled ‘Database access’, Article 21 of that directive states, in paragraphs 1 and 2:  
‘1.      Each Member State shall ensure access for all creditors from all Member States to databases used in that Member State for assessing the creditworthiness of consumers and for the sole purpose of monitoring consumers’ compliance with the credit obligations over the life of the credit agreement. The conditions for such access shall be non-discriminatory.  
2.      Paragraph 1 shall apply both to databases which are operated by private credit bureaux or credit reference agencies and to public registers.’  
   
Regulation (EU) 2015/848  
8        Under recital 76 of Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (OJ 2015 L 141, p. 19):  
‘In order to improve the provision of information to relevant creditors and courts and to prevent the opening of parallel insolvency proceedings, Member States should be required to publish relevant information in cross-border insolvency cases in a publicly accessible electronic register. In order to facilitate access to that information for creditors and courts domiciled or located in other Member States, this Regulation should provide for the interconnection of such insolvency registers via the European e-Justice Portal. …’  
9        Entitled ‘Responsibilities of Member States regarding the processing of personal data in national insolvency registers’, Article 79 of that regulation provides, in paragraphs 4 and 5 thereof:  
‘4.      Member States shall be responsible, in accordance with Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], for the collection and storage of data in national databases and for decisions taken to make such data available in the interconnected register that can be consulted via the European e-Justice Portal.  
5.      As part of the information that should be provided to data subjects to enable them to exercise their rights, and in particular the right to the erasure of data, Member States shall inform data subjects of the accessibility period set for personal data stored in insolvency registers.’  
   
The GDPR  
10      Under recitals 10, 11, 47, 50, 98, 141 and 143 of the GDPR:  
‘(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
(11)      Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.  
…  
(47)      The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. …  
…  
(50)      The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. … In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.  
…  
(98)      Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.  
…  
(141)      Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. …  
…  
(143)      … [E]ach natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State’s procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.  
Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. …’  
11      Entitled ‘Principles relating to processing of personal data’, Article 5 of that regulation is worded as follows:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
…  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
…  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
12      Headed ‘Lawfulness of processing’, Article 6 of that regulation provides:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
…  
4.      Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject’s consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:  
(a)      any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;  
(b)      the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;  
(c)      the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;  
(d)      the possible consequences of the intended further processing for data subjects;  
(e)      the existence of appropriate safeguards, which may include encryption or pseudonymisation.’  
13      Entitled ‘Right to erasure (“right to be forgotten”)’, Article 17 of the GDPR provides, in paragraph 1 thereof:  
‘The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:  
…  
(c)      the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);  
(d)      the personal data have been unlawfully processed;  
…’   
14      Entitled ‘Right to object’, Article 21 of that regulation provides, in paragraphs 1 and 2 thereof:  
‘1.      The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.  
2.      Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.’  
15      Entitled ‘Codes of conduct’, Article 40 of that regulation provides, in paragraphs 1, 2 and 5 thereof:  
‘1.      The Member States, the supervisory authorities, the Board and the [European] Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.  
2.      Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:  
(a)      fair and transparent processing;  
(b)      the legitimate interests pursued by controllers in specific contexts;  
(c)      the collection of personal data;  
…  
5.      Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.’  
16      Entitled ‘Supervisory authority’, Article 51 of the GDPR provides, in paragraph 1 thereof:  
‘Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (“supervisory authority”).’  
17      Entitled ‘Independence’, Article 52 of that regulation provides, in paragraphs 1, 2 and 4 thereof:  
‘1.      Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.  
2.      The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.  
…  
4.      Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.’  
18      Article 57(1) of that regulation, that article being entitled ‘Tasks’, provides:  
‘Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:  
(a)      monitor and enforce the application of this Regulation;  
…  
(f)      handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;  
…’  
19      Entitled ‘Powers’, Article 58 of the GDPR lists, in paragraph 1, the investigative powers available to each supervisory authority and, in paragraph 2, the corrective powers that it may have.  
20      Under the heading ‘Right to lodge a complaint with a supervisory authority’, Article 77 of that regulation states:  
‘1.      Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.  
2.      The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.’  
21      Under the heading ‘Right to an effective judicial remedy against a supervisory authority’, Article 78 of the GDPR provides, in paragraphs 1 and 2 thereof:  
‘1.      Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.  
2.      Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.’  
22      Entitled ‘Right to an effective judicial remedy against a controller or processor’, Article 79 of the GDPR provides, in paragraph 1 thereof:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’  
   
German law  
23      Under Paragraph 9(1) of the Insolvenzordnung (Insolvency Code) of 5 October 1994 (BGBl. 1994 I, p. 2866), in the version applicable to the facts in the main proceedings:  
‘Public notification shall take place by means of centralised publication at national level on the internet; this may be done in extract form. The debtor must be precisely identified, and, in particular, his or her address and business sector must be stated. Notification is deemed to have been effected after two further days following the day of publication have elapsed.’  
24      Paragraph 3 of the Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (Regulation on public notifications in insolvency proceedings on the internet) of 12 February 2002 (BGBl. I, p. 677; ‘the InsoBekV’) stipulates, in subparagraphs 1 and 2 thereof:  
‘(1)      The publication of data from insolvency proceedings, including preliminary insolvency proceedings, in an electronic information and communication system shall be erased no later than six months after the insolvency proceedings are terminated or the order discontinuing the insolvency proceedings becomes final. If the proceedings are not opened, the period shall begin to run from the date on which the published protective measures are lifted.  
(2)      The first sentence of subparagraph 1 shall apply to publications in the proceedings for a discharge from remaining debts, including the order pursuant to Paragraph 289 of the Insolvency Code, subject to the proviso that the period begins to run from the date on which the decision on discharge from remaining debts becomes final.’  
   
The disputes in the main proceedings and the questions referred for a preliminary ruling  
25      In the context of insolvency proceedings concerning them, UF and AB were granted early discharge from remaining debts by judicial decisions delivered on 17 December 2020 and 23 March 2021 respectively. In accordance with Paragraph 9(1) of the Insolvenzordnung and Paragraph 3(1) and (2) of the InsoBekV, the official publication of those decisions on the internet was discontinued after six months.  
26      SCHUFA is a private credit information agency, which records and stores information from public registers in its own databases, in particular information relating to the discharge from remaining debts. It deletes that information three years after registration, in accordance with the code of conduct drawn up in Germany by the association of agencies providing credit information and approved by the competent supervisory authority.  
27      UF and AB applied to SCHUFA to have the entries relating to the decisions to discharge their remaining debts deleted. That agency refused to accede to their requests, after explaining that its activity was carried out in compliance with the GDPR and that the six-month deletion period provided for in Paragraph 3(1) of the InsoBekV did not apply to it.  
28      UF and AB each lodged a complaint with the HBDI as the competent supervisory authority.  
29      In decisions issued on 1 March 2021 and 9 July 2021 respectively, the HBDI found that SCHUFA’s data processing was lawful.  
30      UF and AB each brought an action against the decision of the HBDI before the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), the referring court. In support of their actions, they argued that the HBDI was obliged, within the scope of its duties and powers, to take measures in respect of SCHUFA to enforce deletion of the entries concerning them.  
31      In its defence, the HBDI argued that the actions should be dismissed.  
32      First, the HBDI argued that the right to lodge a complaint, provided for in Article 77(1) of the GDPR, is conceived solely as a right of petition. Thus, judicial review would be confined to examining whether the supervisory authority handled the complaint and informed the complainant of the progress and outcome of that complaint. By contrast, it is not the responsibility of the court hearing the case to review the substantive correctness of the decision handed down in response to the complaint.  
33      Secondly, the HBDI emphasised that data to which credit information agencies have access may be stored for as long as is necessary for the purposes for which they were stored. In the absence of regulation by the national legislature, codes of conduct have been adopted by the supervisory authorities, and the one drawn up by the association of credit information agencies provides for the deletion of such data exactly three years after entry in the file.  
34      In that regard, in the first place, the referring court considers it necessary to clarify the legal nature of the decision made by the supervisory authority after receiving a complaint under Article 77(1) of the GDPR.  
35      In particular, that court has doubts about the HBDI’s line of argument, since it would undermine the effectiveness of the judicial remedy referred to in Article 78(1) of the GDPR. In addition, having regard to the objective pursued by that regulation, which is to ensure, in the implementation of Articles 7 and 8 of the Charter, effective protection of fundamental rights and freedoms of natural persons, Articles 77 and 78 of the GDPR cannot be interpreted restrictively.  
36      That court advocates an interpretation according to which the decision taken on the merits by the supervisory authority must be subject to full judicial review. However, that authority has both a degree of latitude and discretionary power, and may only be required to act where lawful options cannot be identified.  
37      In the second place, the referring court raises the question, in two respects, of the lawfulness of the storage by credit information agencies of data relating to a person’s solvency from public registers, such as the insolvency register.  
38      First, there are doubts as to the lawfulness of a private agency such as SCHUFA storing data transferred from public registers in its own databases.  
39      First of all, that storage does not take place in relation to a specific reason, but rather in the event that their contractual partners ask them for such information, and ultimately results in the data being retained, especially if the data have already been deleted from the public register because the retention period has expired.  
40      Furthermore, processing and therefore retention of data is authorised only if one of the conditions set out in Article 6(1) of the GDPR is met. In this case, only the condition set out in point (f) of the first subparagraph of Article 6(1) of the GDPR is relevant. It is doubtful whether a credit information agency such as SCHUFA is pursuing a legitimate interest within the meaning of that provision.  
41      Lastly, SCHUFA is only one of several credit information agencies and, consequently, data are often stored in multiple databases in Germany, entailing a massive encroachment on the fundamental right under Article 7 of the Charter.  
42      Secondly, even supposing that the storage by private agencies of data from public registers were lawful as such, the question of the possible duration of such storage arises.  
43      In that regard, the referring court is of the view that those private agencies should be required to comply with the six-month time limit laid down in Paragraph 3 of the InsoBekV relating to the retention in the insolvency register of decisions to discharge remaining debts. Thus, data which must be deleted from the public register would also have to be simultaneously deleted at all private credit information agencies which have stored those data.  
44      Moreover, the question arises as to whether a code of conduct approved in accordance with Article 40 of the GDPR, which provides for a three-year deletion period for the entry relating to the discharge from remaining debts, should be taken into account in the balancing exercise to be carried out in the context of the assessment under point (f) of the first subparagraph of Article 6(1) of the GDPR.  
45      In those circumstances, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 77(1) of [the GDPR], read in conjunction with Article 78(1) thereof, to be understood as meaning that the outcome that the supervisory authority reaches and notifies to the data subject:  
–        has the character of a decision on a petition? This would mean that judicial review of a decision on a complaint taken by a supervisory authority in accordance with Article 78(1) of that regulation is, in principle, limited to the question of whether the authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation,  
or  
–        is to be understood as a decision on the merits taken by a public authority? This would mean that a decision on a complaint taken by a supervisory authority would be subject to a full substantive review by the court in accordance with Article 78(1) of that regulation, whereby, in individual cases – for example where discretion is reduced to zero – the supervisory authority may also be obliged by the court to take a specific measure within the meaning of Article 58 of that same regulation?  
(2)      Is the storage of data at a private credit information agency, where personal data from a public register, such as the “national databases” within the meaning of Article 79(4) and (5) of Regulation [2015/848] are stored without a specific reason in order to be able to provide information in the event of a request, compatible with Articles 7 and 8 of the [Charter]?  
(3)      (a)      Are private databases (in particular databases of a credit information agency) which exist in parallel with, and are set up in addition to, the State databases and in which the data from the latter (  
in casu  
, insolvency announcements) are stored for longer than the period provided for within the narrow framework of Regulation 2015/848, read in conjunction with the national law, permissible in principle?  
(b)      If Question 3a is answered in the affirmative, does it follow from the “right to be forgotten” under Article 17(1)(d) of [the GDPR] that such data must be deleted where the processing period provided for in respect of the public register has expired?  
(4)      In so far as point (f) of [the first subparagraph of] Article 6(1) of [the GDPR] enters into consideration as the sole legal basis for the storage of data at private credit information agencies with regard to data also stored in public registers, is a credit information agency already to be regarded as pursuing a legitimate interest in the case where it imports data from the public register without a specific reason so that those data are then available in the event of a request?  
(5)      Is it permissible for codes of conduct which have been approved by the supervisory authorities in accordance with Article 40 of [the GDPR], and which provide for time limits for review and erasure that exceed the retention periods for public registers, to suspend the balancing of interests prescribed under point (f) of [the first subparagraph of] Article 6(1) of that regulation?’  
46      By decision of the President of the Court of 11 February 2022, Cases C-26/22 and C-64/22 were joined for the purposes of the written and oral parts of the procedure and of the judgment.  
   
Consideration of the questions referred  
   
The first question  
47      By its first question, the referring court asks, in essence, whether Article 78(1) of the GDPR must be interpreted as meaning that judicial review of a decision on a complaint taken by a supervisory authority is limited to the question whether that authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation, or whether that decision is subject to a full judicial review, including the power of the court seised to require the supervisory authority to take a specific measure.  
48      In order to answer that question, it should be borne in mind, as a preliminary point, that the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 22 June 2023,   
Pankki S  
,   
C-579/21, EU:C:2023:501, paragraph 38 and the case-law cited).  
49      In respect of the wording of Article 78(1) of the GDPR, that provision provides that, without prejudice to any other administrative or non-judicial remedy, each natural or legal person is to have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.  
50      In this respect, it should be noted from the outset that, in the present case, the decisions adopted by the HBDI constitute legally binding decisions within the meaning of Article 78(1) of the GDPR. After examining the merits of the complaints lodged with it, that authority found that the processing of personal data challenged by the applicants in the main proceedings was lawful under the GDPR. Moreover, the legally binding nature of those decisions is confirmed by recital 143 of that regulation, according to which the dismissal or rejection of a complaint by a supervisory authority constitutes a decision producing legal effects with regard to the complainant.  
51      It should also be noted that that provision, read in the light of recital 141 of the GDPR, explicitly states that any data subject has the right to an ‘effective’ judicial remedy, in accordance with Article 47 of the Charter.  
52      Thus, the Court has already held that it follows from Article 78(1) of the GDPR, read in the light of recital 143 of that regulation, that courts seised of an action against a decision of a supervisory authority should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them (judgment of 12 January 2023,   
Nemzeti Adatvédelmi és Információszabadság Hatóság  
, C-132/21, EU:C:2023:2, paragraph 41).  
53      Therefore, Article 78(1) of the GDPR cannot be interpreted as meaning that judicial review of a decision on a complaint taken by a supervisory authority is limited to the question of whether the authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation. On the contrary, for a judicial remedy to be ‘effective’, as required by that provision, such a decision must be subject to full judicial review.  
54      That interpretation is supported by the context of Article 78(1) of the GDPR and by the objectives and purpose of the regulation.  
55      As regards the context surrounding that provision, it is important to note that, in accordance with Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data (judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 107).  
56      In particular, under Article 57(1)(f) of the GDPR, each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that data subject considers that the processing of his or her personal data infringes the regulation, and is required to examine the nature of that complaint as necessary. The supervisory authority must deal with such a complaint with all due diligence (judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 109).  
57      In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. Where, following its investigation, such an authority finds an infringement of the provisions of that regulation, it is required to react appropriately in order to remedy the shortcoming found. To that end, Article 58(2) of that regulation lists the various corrective measures that the supervisory authority may adopt (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 111).  
58      It follows, as the Advocate General observed in point 42 of his Opinion, that the complaints procedure, which is not similar to that of a petition, is designed as a mechanism capable of effectively safeguarding the rights and interests of data subjects.  
59      However, in view of the wide-ranging powers vested in the supervisory authority under the GDPR, the requirement for effective judicial protection would not be met if decisions concerning the exercise by such a supervisory authority of powers of investigation or the adoption of corrective measures were subject only to limited judicial review.  
60      The same applies to decisions rejecting a complaint, as Article 78(1) of the GDPR makes no distinction according to the nature of the decision adopted by the supervisory authority.  
61      As regards the objectives pursued by the GDPR, it is apparent, in particular, from recital 10 thereof that the aim of that regulation is to ensure a high level of protection of natural persons with regard to the processing of personal data within the European Union. Moreover, recital 11 of that regulation states that effective protection of such data requires the strengthening of the rights of data subjects.  
62      If Article 78(1) of that regulation were to be interpreted as meaning that the judicial review referred to therein is limited to verifying whether the supervisory authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation, the attainment of the objectives and the pursuit of the purpose of the regulation would necessarily be compromised.  
63      Furthermore, an interpretation of that provision according to which a decision on a complaint adopted by a supervisory authority is subject to full judicial review does not call into question the guarantees of independence enjoyed by supervisory authorities, nor the right to an effective judicial remedy against a controller or processor.  
64      In the first place, it is true that, in accordance with Article 8(3) of the Charter, compliance with the rules on the protection of personal data is subject to control by an independent authority. In that context, Article 52 of the GDPR specifies, in particular, that each supervisory authority is to act with complete independence in performing its tasks and exercising its powers in accordance with that regulation (paragraph 1), that, in the performance of their tasks and exercise of their powers, the member or members of each supervisory authority are to remain free from external influence (paragraph 2), and that each Member State is to ensure that each supervisory authority has the resources necessary for the effective performance of its duties and the exercise of its powers (paragraph 4).  
65      However, those guarantees of independence are in no way compromised by the fact that the legally binding decisions of a supervisory authority are subject to full judicial review.  
66      In the second place, as regards the right to an effective judicial remedy against a controller or processor provided for in Article 79(1) of the GDPR, it should be noted that, according to the case-law of the Court, the remedies provided for, respectively, in Article 78(1) and Article 79(1) of that regulation may be exercised concurrently with and independently of each other (judgment of 12 January 2023,   
Nemzeti Adatvédelmi és Információszabadság Hatóság  
, C-132/21, EU:C:2023:2, paragraph 35 and operative part). In that context, the Court has held, inter alia, that making several remedies available strengthens the objective set out in recital 141 of that regulation of guaranteeing for every data subject who considers that his or her rights under that regulation are infringed the right to an effective judicial remedy in accordance with Article 47 of the Charter (judgment of 12 January 2023,   
Nemzeti Adatvédelmi és Információszabadság Hatóság  
, C-132/21, EU:C:2023:2, paragraph 44).  
67      Therefore, and even though it is for the Member States, in accordance with the principle of procedural autonomy, to lay down the detailed rules for the coordination of those remedies (judgment of 12 January 2023,   
Nemzeti Adatvédelmi és Információszabadság Hatóság  
, C-132/21, EU:C:2023:2, paragraph 45 and operative part), the existence of the right to an effective judicial remedy against a controller or processor, provided for in Article 79(1) of the GDPR, does not affect the scope of the judicial review exercised, in the context of an action brought under Article 78(1) of that regulation, over a decision on a complaint adopted by a supervisory authority.  
68      However, it should be added that, while, as pointed out in paragraph 56 of this judgment, the supervisory authority must deal with a complaint with all due diligence, that authority has, as regards the remedies listed in Article 58(2) of the GDPR, a margin of discretion as to the choice of appropriate and necessary means (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 112).  
69      While the national court hearing an action under Article 78(1) of the GDPR must, as noted in paragraph 52 of this judgment, have full jurisdiction to examine all questions of fact and law relating to the dispute concerned, the guarantee of effective judicial protection does not imply that it is entitled to substitute its assessment of the choice of appropriate and necessary remedies for that of that authority, but requires that court to examine whether the supervisory authority has complied with the limits of its discretion.  
70      In the light of all the foregoing considerations, the answer to the first question is that Article 78(1) of the GDPR must be interpreted as meaning that a decision on a complaint adopted by a supervisory authority is subject to full judicial review.  
   
The second to fifth questions  
71      By its second to fifth questions, which it is appropriate to consider together, the referring court asks, in essence,  
–        whether Article 5(1)(a) of the GDPR, read in conjunction with point (f) of the first subparagraph of Article 6(1) of that regulation, must be interpreted as precluding a practice of private credit information agencies consisting in retaining, in their own databases, information from a public register relating to the grant of a discharge from remaining debts in favour of natural persons, and in deleting that information after a period of three years, in accordance with a code of conduct within the meaning of Article 40 of that regulation, whereas the period of retention of that information in the public register is six months, and,  
–        whether Article 17(1)(c) and (d) of the GDPR must be interpreted as meaning that a private credit information agency which has acquired information relating to the grant of a discharge from remaining debts from a public register is obliged to delete that information.  
   
Article 5(1)(a) of the GDPR  
72      Article 5(1)(a) of the GDPR provides that personal data is to be processed lawfully, fairly and in a transparent manner in relation to the data subject.  
73      In that context, the first subparagraph of Article 6(1) of that regulation sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being regarded as such, processing must fall within one of the cases provided for in that provision (judgment of 4 July 2023,   
Meta Platforms and Others   
(General terms of use of a social network)  
, C-252/21, EU:C:2023:537, paragraph 90 and the case-law cited).  
74      In the present case, it is common ground that the lawfulness of the processing of personal data at issue in the main proceedings must be assessed solely in the light of point (f) of the first subparagraph of Article 6(1) of the GDPR. Under that provision, the processing of personal data is lawful only if and to the extent that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
75      Accordingly, that provision lays down three cumulative conditions for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or freedoms and fundamental rights of the person concerned by the data protection do not take precedence (judgment of 4 July 2023,   
Meta Platforms and Others   
(General terms of use of a social network)  
, C-252/21, EU:C:2023:537, paragraph 106 and the case-law cited).  
76      As regards, first, the condition relating to the pursuit of a ‘legitimate interest’, in the absence of a definition of that concept in the GDPR, it should be emphasised, as the Advocate General observed in point 61 of his Opinion, that a wide range of interests is, in principle, capable of being regarded as legitimate.  
77      Second, with regard to the condition that the processing of personal data be necessary for the purposes of the legitimate interests pursued, that condition requires the referring court to ascertain that the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (judgment of 4 July 2023,   
Meta Platforms and Others   
(General terms of use of a social network)  
, C-252/21, EU:C:2023:537, paragraph 108 and the case-law cited).  
78      In that context, it should also be recalled that the condition relating to the need for processing must be examined in conjunction with the ‘data minimisation’ principle enshrined in Article 5(1)(c) of the GDPR, in accordance with which personal data must be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’ (judgment of 4 July 2023,   
Meta Platforms and Others   
(General terms of use of a social network)  
, C-252/21, EU:C:2023:537, paragraph 109 and the case-law cited).  
79      Third, with regard to the condition that the interests or fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interests of the controller or of a third party, the Court has already held that that condition entails a balancing of the opposing rights and interests at issue which depends in principle on the specific circumstances of the particular case and that, consequently, it is for the referring court to carry out that balancing exercise, taking account of those specific circumstances (judgment of 4 July 2023,   
Meta Platforms and Others   
(General terms of use of a social network)  
, C-252/21, EU:C:2023:537, paragraph 110 and the case-law cited).  
80      Furthermore, as can be seen from recital 47 of the GDPR, the interests and fundamental rights of the data subject may in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing (judgment of 4 July 2023,   
Meta Platforms and Others   
(General terms of use of a social network)  
, C-252/21, EU:C:2023:537, paragraph 112).  
81      While it is therefore ultimately for the national court to assess whether, in relation to the processing of personal data at issue in the main proceedings, the three conditions referred to in paragraph 75 of this judgment are satisfied, it is open to the Court, when giving a preliminary ruling on a reference, to give clarifications to guide the national court in that determination (see, to that effect, judgment of 20 October 2022,   
Digi  
, C-77/21, EU:C:2022:805, paragraph 39 and the case-law cited).  
82      In this case, with regard to the pursuit of a legitimate interest, SCHUFA argues that credit information agencies process the data necessary for the assessment of the creditworthiness of persons or undertakings in order to be able to make that information available to their contractual partners. In addition to protecting the economic interests of agencies wishing to enter into credit-linked contracts, the determination of creditworthiness and the provision of information on creditworthiness form the basis of credit and the economy’s ability to function. The activity of those agencies also helps to clarify the business requirements of persons involved in credit-related transactions as the report allows a quick and non-bureaucratic examination of those transactions.  
83      In that regard, while the processing of personal data such as that at issue in the main proceedings serves SCHUFA’s economic interests, that processing also serves to pursue the legitimate interest of SCHUFA’s contractual partners, who intend to conclude credit agreements with individuals, in being able to assess the creditworthiness of those individuals, and thus the interests of the credit sector from a socio-economic point of view.  
84      In the case of consumer credit agreements, Article 8 of Directive 2008/48, read in the light of recital 28 thereof, states that, before the conclusion of the credit agreement, the creditor is required to assess the consumer’s creditworthiness on the basis of sufficient information, including, where appropriate, information from public and private databases.  
85      Furthermore, as regards consumer credit agreements relating to residential immovable property, it follows from Articles 18(1) and 21(1) of Directive 2014/17, read in the light of recitals 55 and 59 thereof, that the creditor must make a thorough assessment of the consumer’s creditworthiness and that he or she must have access to credit databases, the consultation of such databases being a useful element for the purposes of that assessment.  
86      It should be added that the obligation to assess the creditworthiness of consumers, as laid down in Directives 2008/48 and 2014/17, is intended not only to protect the credit applicant but also, as pointed out in recital 26 of Directive 2008/48, to ensure the proper functioning of the credit system as a whole.  
87      However, the data processing must also be necessary in order to achieve the legitimate interests pursued by the controller or by a third party and the interests or fundamental freedoms and rights of the data subject must not override those interests. In the context of that balancing of the opposing rights and interests at issue, namely, those of the controller and of the third parties involved, on the one hand, and those of the data subject, on the other, account must be taken, as has been noted in paragraph 80 of this judgment, in particular of the reasonable expectations of the data subject as well as the scale of the processing at issue and its impact on that person (see judgment of 4 July 2023,   
Meta Platforms and Others   
(General terms of use of a social network)  
, C-252/21, EU:C:2023:537, paragraph 116).  
88      As regards point (f) of the first subparagraph of Article 6(1) of the GDPR, the Court has held that that provision must be interpreted as meaning that processing can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of that provision, only if such processing is carried out in so far as is strictly necessary for the purposes of that legitimate interest and if it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of the persons concerned by the processing at issue do not override that legitimate interest of the controller or of a third party (see, to that effect, judgments of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 30, and of 4 July 2023,   
Meta Platforms and Others   
(General terms of use of a social network)  
, C-252/21, EU:C:2023:537, paragraph 126).  
89      In that context, the referring court refers to two aspects of the processing of personal data at issue in the main proceedings. In the first place, that processing would involve storing the data in a variety of ways, namely not only in a public register but also in the databases of the credit information agencies, it being specified that those agencies store the data not in relation to a specific reason but rather in the event that their contractual partners ask them for such information. In the second place, those agencies store the data for three years, on the basis of a code of conduct within the meaning of Article 40 of the GDPR, whereas the national legislation provides for a storage period of only six months in the case of the public register.  
90      With regard to the first of those aspects, SCHUFA argues that it would be impossible to provide information in a timely manner if a credit information agency had to wait for a specific request before it could start collecting data.  
91      In that regard, it is for the referring court to ascertain whether the storage of the data at issue by SCHUFA in its own databases is limited to what is strictly necessary in order to achieve the legitimate interest pursued, when the data at issue can be consulted in the public register and without a commercial undertaking having requested information in a specific case. If this were not the case, the storage of such data by SCHUFA could not be considered necessary for the period during which the data are made available to the public.  
92      As regards the length of time for which the data are stored, it must be held that the examinations of the second and third conditions referred to in paragraph 75 of this judgment merge in so far as the assessment of whether, in the present case, the legitimate interests pursued by the processing of personal data at issue in the main proceedings cannot reasonably be achieved by a shorter period for storing the data requires a balancing of the opposing rights and interests at issue.  
93      As regards the balancing of the legitimate interests pursued, it should be noted that, in so far as the analysis provided by a credit information agency makes it possible to assess objectively and reliably the creditworthiness of the potential customers of the contractual partners of the agency supplying that credit information, it makes it possible to compensate for disparities in information and therefore to reduce the risks of fraud and other uncertainties.  
94      On the other hand, as regards the rights and interests of the data subject, the processing of data relating to the granting of a discharge from remaining debts, by a credit information agency, such as the storage, analysis and communication of such data to a third party, constitutes a serious interference with the fundamental rights of the data subject, enshrined in Articles 7 and 8 of the Charter. Such data is used as a negative factor when assessing the data subject’s creditworthiness and therefore constitutes sensitive information about his or her private life (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 98). The processing of such data is likely to be considerably detrimental to the interests of the data subject in so far as such disclosure is likely to make it significantly more difficult for him or her to exercise his or her freedoms, particularly where basic needs are concerned.  
95      Furthermore, as the Commission has pointed out, the longer the data in question is stored by credit information agencies, the greater the impact on the interests and private life of the data subject and the greater the requirements relating to the lawfulness of the storage of that information.  
96      It should also be noted that, as stated in recital 76 of Regulation 2015/848, the purpose of a public insolvency register is to improve the provision of information to creditors as well as to the courts concerned. In that context, Article 79(5) of that regulation merely provides that Member States are to inform data subjects of the accessibility period set for personal data stored in insolvency registers, without setting a time limit for the retention of such data. By contrast, it is apparent from Article 79(4) of the GDPR that Member States are responsible, in accordance with that regulation, for the collection and storage of personal data in national databases. The retention period for such data must then be set in compliance with the GDPR.  
97      In this case, the German legislature provides that information relating to the granting of a discharge from remaining debts is kept in the insolvency register for only six months. It therefore considers that, after the expiry of a six-month period, the rights and interests of the data subject take precedence over those of the public to have access to that information.  
98      Moreover, as the Advocate General observed in point 75 of his Opinion, the discharge from remaining debts is intended to allow the person who benefits from it to re-enter economic life and is therefore generally of existential importance to that person. The attainment of that objective would be jeopardised if credit information agencies could, for the purposes of assessing the economic situation of a person, retain data relating to a discharge from remaining debts and use such data after they have been deleted from the public insolvency register, in so far as those data are still used as a negative factor when assessing the solvency of such a person.  
99      In those circumstances, the interests of the credit sector in having access to information on a discharge from remaining debts cannot justify the processing of personal data such as that at issue in the main proceedings beyond the period for which the data are kept in the public insolvency register, so that the retention of those data by a credit information agency cannot be based on point (f) of the first subparagraph of Article 6(1) of the GDPR as regards the period following the deletion of those data from a public insolvency register.  
100    As regards the six-month period during which the data in question are also available in that public register, it should be noted that, although the effects of parallel storage of those data in the databases of such agencies may be regarded as less serious than after the six months have elapsed, such storage nevertheless constitutes an interference with the rights enshrined in Articles 7 and 8 of the Charter. In that regard, the Court has already held that the presence of the same personal data in several sources reinforces the interference with the individual’s right to privacy (see judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraphs 86 and 87). It is for the referring court to weigh up the interests involved and the impact on the data subject concerned, in order to establish whether the parallel storage of those data by private credit information agencies can be regarded as being limited to what is strictly necessary, as required by the case-law of the Court cited in paragraph 88 of this judgment.  
101    Finally, with regard to the existence, as in the present case, of a code of conduct providing that a credit information agency must delete data relating to a release from remaining debts after a period of three years, it should be recalled that, in accordance with Article 40(1) and (2) of the GDPR, codes of conduct are intended to contribute to the proper application of that regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises. Thus, associations and other bodies representing categories of data controllers or processors may draw up, amend or extend codes of conduct, for the purpose of specifying the application of that regulation, such as with regard to fair and transparent processing, the legitimate interests pursued by controllers in specific contexts and the collection of personal data.  
102    In addition, under Article 40(5) of the GDPR, a draft code is to be submitted to the competent supervisory authority, which is to approve it if it finds that it provides sufficient appropriate safeguards.  
103    In the present case, the code of conduct at issue in the main proceedings was drawn up by the association of German credit information agencies and approved by the competent supervisory authority.  
104    That being so, while, in accordance with Article 40(1) and (2) of the GDPR, a code of conduct is intended to contribute to the proper application of that regulation and to specify the application of that regulation, the fact remains, as the Advocate General observed in points 103 and 104 of his Opinion, that the conditions for the lawfulness of the processing of personal data laid down by such a code cannot differ from the conditions laid down in Article 6(1) of the GDPR.  
105    Thus, a code of conduct that leads to an assessment different from that obtained pursuant to point (f) of the first subparagraph of Article 6(1) of the GDPR cannot be taken into account in the balance of interests under that provision.  
   
Article 17 of the GDPR  
106    Lastly, the referring court raises the question, in essence, of the obligations incumbent on a credit information agency under Article 17 of the GDPR.  
107    In that regard, it should be borne in mind that, under Article 17(1)(d) of the GDPR, to which the referring court refers, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay where the personal data have been unlawfully processed.  
108    Therefore, according to the clear wording of that provision, if the national court were to conclude from its assessment of the lawfulness of the processing of personal data at issue in the main proceedings that that processing was not lawful, it would be incumbent on the controller, in this case SCHUFA, to delete the data concerned as soon as possible. This would be the case, as noted in paragraph 99 of this judgment, in respect of the processing of personal data beyond the six-month period for which the data are kept in the public insolvency register.  
109    As regards the processing at issue during the six-month period in which the data are available in the public insolvency register, if the referring court were to conclude that the processing complied with point (f) of the first subparagraph of Article 6(1) of the GDPR, Article 17(1)(c) of that regulation would apply.  
110    That provision establishes the right to erasure of personal data where the data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no ‘overriding legitimate grounds for the processing’. Under the latter provision, the data subject is to have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of the first subparagraph of Article 6(1) of the GDPR. The controller is no longer required to process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.  
111    As the Advocate General observed in point 93 of his Opinion, it follows from a combined reading of those provisions that the data subject enjoys a right to object to processing and a right to erasure, unless there are overriding legitimate grounds which take precedence over the interests and rights and freedoms of that person within the meaning of Article 21(1) of the GDPR, which it is for the controller to demonstrate.  
112    Consequently, if the controller fails to provide such proof, the data subject is entitled to request the erasure of the data on the basis of Article 17(1)(c) of the GDPR, where he or she objects to the processing in accordance with Article 21(1) of that regulation. It is for the referring court to examine whether, exceptionally, there are overriding legitimate grounds capable of justifying the processing in question.  
113    In the light of all the foregoing considerations, the second to fifth questions should be answered as follows:  
–        Article 5(1)(a) of the GDPR, read in conjunction with point (f) of the first subparagraph of Article 6(1) of that regulation, must be interpreted as precluding a practice of private credit information agencies consisting in retaining, in their own databases, information from a public register relating to the grant of a discharge from remaining debts in favour of natural persons in order to be able to provide information on the solvency of those persons, for a period extending beyond that during which the data are kept in the public register;  
–        Article 17(1)(c) of the GDPR must be interpreted as meaning that the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where he or she objects to the processing pursuant to Article 21(1) of that regulation and there are no overriding legitimate grounds capable of justifying, exceptionally, the processing in question;  
–        Article 17(1)(d) of the GDPR must be interpreted as meaning that the controller is required to erase unlawfully processed personal data as soon as possible.  
   
Costs  
114    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
1.        
Article 78(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
must be interpreted as meaning that a decision on a complaint adopted by a supervisory authority is subject to full judicial review.  
2.        
Article 5(1)(a) of Regulation 2016/679, read in conjunction with point (f) of the first subparagraph of Article 6(1) of that regulation,  
must be interpreted as precluding a practice of private credit information agencies consisting in retaining, in their own databases, information from a public register relating to the grant of a discharge from remaining debts in favour of natural persons in order to be able to provide information on the solvency of those persons, for a period extending beyond that during which the data are kept in the public register.  
3.        
Article 17(1)(c) of Regulation 2016/679  
must be interpreted as meaning that the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where he or she objects to the processing pursuant to Article 21(1) of that regulation and there are no overriding legitimate grounds capable of justifying, exceptionally, the processing in question.  
4.        
Article 17(1)(d) of Regulation 2016/679  
must be interpreted as meaning that the controller is required to erase unlawfully processed personal data as soon as possible.

ID: 52f8df9b-3d43-4224-b1e6-664e81d55116

Judgment of 6 Oct 2015, C-362/14 (  
Schrems I  
)  
General data protection law   
 >   
Chapter V - International data transfer   
 >   
Adequacy decision   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
General data protection law   
 >   
Chapter V - International data transfer   
 >   
Adequacy decision   
   
JUDGMENT OF THE COURT (Grand Chamber)  
6 October 2015 (\*)  
(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities)  
In Case C-362/14,  
REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings  
Maximillian Schrems  
v  
Data Protection Commissioner,  
joined party:  
Digital Rights Ireland Ltd,  
THE COURT (Grand Chamber),  
composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), S. Rodin and K. Jürimäe, Presidents of Chambers, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen and C. Lycourgos, Judges,  
Advocate General: Y. Bot,  
Registrar: L. Hewlett, Principal Administrator,  
having regard to the written procedure and further to the hearing on 24 March 2015,  
after considering the observations submitted on behalf of:  
–        Mr Schrems, by N. Travers, Senior Counsel, P. O’Shea, Barrister-at-Law, G. Rudden, Solicitor, and H. Hofmann, Rechtsanwalt,  
–        the Data Protection Commissioner, by P. McDermott, Barrister-at-Law, S. More O’Ferrall and D. Young, Solicitors,  
–        Digital Rights Ireland Ltd, by F. Crehan, Barrister-at-Law, and S. McGarr and E. McGarr, Solicitors,   
–        Ireland, by A. Joyce, B. Counihan and E. Creedon, acting as Agents, and D. Fennelly, Barrister-at-Law,   
–        the Belgian Government, by J.-C. Halleux and C. Pochet, acting as Agents,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,  
–        the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,  
–        the Polish Government, by M. Kamejsza, M. Pawlicka and B. Majczyna, acting as Agents,  
–        the Slovenian Government, by A. Grum and V. Klemenc, acting as Agents,  
–        the United Kingdom Government, by L. Christie and J. Beeko, acting as Agents, and J. Holmes, Barrister,  
–        the European Parliament, by D. Moore, A. Caiola and M. Pencheva, acting as Agents,  
–        the European Commission, by B. Schima, B. Martenczuk, B. Smulders and J. Vondung, acting as Agents,  
–        the European Data Protection Supervisor (EDPS), by C. Docksey, A. Buchta and V. Pérez Asinari, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 23 September 2015,  
gives the following  
Judgment  
1        This request for a preliminary ruling relates to the interpretation, in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’), of Articles 25(6) and 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1) (‘Directive 95/46’), and, in essence, to the validity of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).  
2        The request has been made in proceedings between Mr Schrems and the Data Protection Commissioner (‘the Commissioner’) concerning the latter’s refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd (‘Facebook Ireland’) transfers the personal data of its users to the United States of America and keeps it on servers located in that country.  
   
Legal context  
   
Directive 95/46  
3        Recitals 2, 10, 56, 57, 60, 62 and 63 in the preamble to Directive 95/46 are worded as follows:  
‘(2)      ... data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;   
…  
(10)      … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of Community law; …, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;  
…  
(56)      … cross-border flows of personal data are necessary to the expansion of international trade; … the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; … the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;  
(57)      … on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;  
…  
(60)      … in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;  
…  
(62)      … the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;  
(63)      … such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; ...’  
4        Articles 1, 2, 25, 26, 28 and 31 of Directive 95/46 provide:  
‘  
Article 1  
Object of the Directive  
1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
...  
Article 2  
Definitions  
For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
...  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;  
...  
Article 25  
Principles  
1.      The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.  
2.      The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.  
3.      The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.  
4.      Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.  
5.      At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.  
6.      The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.  
Member States shall take the measures necessary to comply with the Commission’s decision.  
Article 26  
Derogations   
1.       By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:  
(a)      the data subject has given his consent unambiguously to the proposed transfer; or  
(b)      the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject’s request; or  
(c)      the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or  
(d)      the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or  
(e)      the transfer is necessary in order to protect the vital interests of the data subject; or  
(f)       the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.  
2.      Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.  
3.      The Member State shall inform the Commission and the other Member States of the authorisations it grants pursuant to paragraph 2.  
If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2).  
Member States shall take the necessary measures to comply with the Commission’s decision.  
...  
Article 28   
Supervisory authority  
1.      Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.  
These authorities shall act with complete independence in exercising the functions entrusted to them.  
2.      Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals’ rights and freedoms with regard to the processing of personal data.  
3.      Each authority shall in particular be endowed with:  
–        investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,  
–        effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,  
–        the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.  
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.  
4.      Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.  
Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.  
...  
6.      Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.  
...  
Article 31  
...  
2.       Where reference is made to this Article, Articles 4 and 7 of [Council] Decision 1999/468/EC [of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ 1999 L 184, p. 23)] shall apply, having regard to the provisions of Article 8 thereof.  
...’  
   
Decision 2000/520  
5        Decision 2000/520 was adopted by the Commission on the basis of Article 25(6) of Directive 95/46.   
6        Recitals 2, 5 and 8 in the preamble to that decision are worded as follows:  
‘(2)      The Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary.  
…  
(5)      The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States (hereinafter “the Principles”) and the frequently asked questions (hereinafter “the FAQs”) providing guidance for the implementation of the Principles issued by the Government of the United States on 21 July 2000. Furthermore the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs.  
…  
(8)      In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.’  
7        Articles 1 to 4 of Decision 2000/520 provide:  
‘  
Article 1  
1.      For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the “Safe Harbour Privacy Principles” (hereinafter “the Principles”), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter “the FAQs”) issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce:  
(a)      the safe harbour enforcement overview set out in Annex III;  
(b)      a memorandum on damages for breaches of privacy and explicit authorisations in US law set out in Annex IV;  
(c)      a letter from the Federal Trade Commission set out in Annex V;  
(d)      a letter from the US Department of Transportation set out in Annex VI.  
2.      In relation to each transfer of data the following conditions shall be met:  
(a)      the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and  
(b)      the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.  
3.      The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).  
Article 2  
This Decision concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.  
Article 3  
1.      Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:  
(a)      the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or  
(b)      there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.  
The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.  
2.      Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.  
3.      The Member States and the Commission shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States fails to secure such compliance.  
4.      If the information collected under paragraphs 1, 2 and 3 provides evidence that any body responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States is not effectively fulfilling its role, the Commission shall inform the US Department of Commerce and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC with a view to reversing or suspending the present Decision or limiting its scope.  
Article 4  
1.      This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.  
The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.  
2.      The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.’  
8        Annex I to Decision 2000/520 is worded as follows:  
‘Safe Harbour Privacy Principles  
issued by the US Department of Commerce on 21 July 2000  
... the Department of Commerce is issuing this document and Frequently Asked Questions (“the Principles”) under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of “adequacy” it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. …  
Decisions by organisations to qualify for the safe harbour are entirely voluntary, and organisations may qualify for the safe harbour in different ways. ...  
Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation; or (c) if the effect of the Directive [or] Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organisations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or US law, organisations are expected to opt for the higher protection where possible.  
...’  
9        Annex II to Decision 2000/520 reads as follows:  
‘Frequently Asked Questions (FAQs)  
...  
FAQ 6 — Self-Certification  
Q:        
How does an organisation self-certify that it adheres to the Safe Harbour Principles?   
A:      Safe harbour benefits are assured from the date on which an organisation self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.  
To self-certify for the safe harbour, organisations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organisation that is joining the safe harbour, that contains at least the following information:  
1.      name of organisation, mailing address, e-mail address, telephone and fax numbers;  
2.      description of the activities of the organisation with respect to personal information received from the [European Union]; and  
3.      description of the organisation’s privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbour, (d) the specific statutory body that has jurisdiction to hear any claims against the organisation regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programmes in which the organisation is a member, (f) method of verification (e.g. in-house, third party) …, and (g) the independent recourse mechanism that is available to investigate unresolved complaints.  
Where the organisation wishes its safe harbour benefits to cover human resources information transferred from the [European Union] for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organisation arising out of human resources information that is listed in the annex to the Principles. ...  
The Department (or its designee) will maintain a list of all organisations that file such letters, thereby assuring the availability of safe harbour benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. ...  
...  
FAQ 11 — Dispute Resolution and Enforcement  
Q:        
How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organisation’s persistent failure to comply with the Principles be handled?   
A:      The Enforcement Principle sets out the requirements for safe harbour enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle’s requirements. Organisations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programmes that incorporate the Safe Harbour Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorised representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle’s requirements are additional to the requirements set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.  
Recourse Mechanisms  
Consumers should be encouraged to raise any complaints they may have with the relevant organisation before proceeding to independent recourse mechanisms. ...  
...  
FTC Action  
The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organisations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbour Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. ...  
…’  
10      Annex IV to Decision 2000/520 states:  
‘Damages for Breaches of Privacy, Legal Authorisations and Mergers and Takeovers in US Law  
This responds to the request by the European Commission for clarification of US law with respect to (a) claims for damages for breaches of privacy, (b) “explicit authorisations” in US law for the use of personal information in a manner inconsistent with the safe harbour principles, and (c) the effect of mergers and takeovers on obligations undertaken pursuant to the safe harbour principles.  
...  
B.      Explicit Legal Authorisations   
The safe harbour principles contain an exception where statute, regulation or case-law create “conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorisation”. Clearly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law. As for explicit authorisations, while the safe harbour principles are intended to bridge the differences between the US and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. The limited exception from strict adherence to the safe harbour principles seeks to strike a balance to accommodate the legitimate interests on each side.  
The exception is limited to cases where there is an explicit authorisation. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorise the particular conduct by safe harbour organisations ... In other words, the exception would not apply where the law is silent. In addition, the exception would apply only if the explicit authorisation conflicts with adherence to the safe harbour principles. Even then, the exception “is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation”. By way of illustration, where the law simply authorises a company to provide personal information to government authorities, the exception would not apply. Conversely, where the law specifically authorises the company to provide personal information to government agencies without the individual’s consent, this would constitute an “explicit authorisation” to act in a manner that conflicts with the safe harbour principles. Alternatively, specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorisation to disclose the information without notice and consent). For example, a statute which authorises doctors to provide their patients’ medical records to health officials without the patients’ prior consent might permit an exception from the notice and choice principles. This authorisation would not permit a doctor to provide the same medical records to health maintenance organisations or commercial pharmaceutical research laboratories, which would be beyond the scope of the purposes authorised by the law and therefore beyond the scope of the exception ... The legal authority in question can be a “stand alone” authorisation to do specific things with personal information, but, as the examples below illustrate, it is likely to be an exception to a broader law which proscribes the collection, use, or disclosure of personal information.  
...’  
   
Communication COM(2013) 846 final  
11      On 27 November 2013 the Commission adopted the communication to the European Parliament and the Council entitled ‘Rebuilding Trust in EU-US Data Flows’ (COM(2013) 846 final) (‘Communication COM(2013) 846 final’). The communication was accompanied by the ‘Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection’, also dated 27 November 2013. That report was drawn up, as stated in point 1 thereof, in cooperation with the United States after the existence in that country of a number of surveillance programmes involving the large-scale collection and processing of personal data had been revealed. The report contained inter alia a detailed analysis of United States law as regards, in particular, the legal bases authorising the existence of surveillance programmes and the collection and processing of personal data by United States authorities.   
12      In point 1 of Communication COM(2013) 846 final, the Commission stated that ‘[c]ommercial exchanges are addressed by Decision [2000/520]’, adding that ‘[t]his Decision provides a legal basis for transfers of personal data from the [European Union] to companies established in the [United States] which have adhered to the Safe Harbour Privacy Principles’. In addition, the Commission underlined in point 1 the increasing relevance of personal data flows, owing in particular to the development of the digital economy which has indeed ‘led to exponential growth in the quantity, quality, diversity and nature of data processing activities’.  
13      In point 2 of that communication, the Commission observed that ‘concerns about the level of protection of personal data of [Union] citizens transferred to the [United States] under the Safe Harbour scheme have grown’ and that ‘[t]he voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement’.  
14      It further stated in point 2 that ‘[t]he personal data of [Union] citizens sent to the [United States] under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the [European Union] and the purposes for which it was transferred to the [United States]’ and that ‘[a] majority of the US internet companies that appear to be more directly concerned by [the surveillance] programmes are certified under the Safe Harbour scheme’.  
15      In point 3.2 of Communication COM(2013) 846 final, the Commission noted a number of weaknesses in the application of Decision 2000/520. It stated, first, that some certified United States companies did not comply with the principles referred to in Article 1(1) of Decision 2000/520 (‘the safe harbour principles’) and that improvements had to be made to that decision regarding ‘structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception’. It observed, secondly, that ‘Safe Harbour also acts as a conduit for the transfer of the personal data of EU citizens from the [European Union] to the [United States] by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes’.  
16      The Commission concluded in point 3.2 that whilst, ‘[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained, ... its revocation would[, however,] adversely affect the interests of member companies in the [European Union] and in the [United States]’. Finally, the Commission added in that point that it would ‘engage with the US authorities to discuss the shortcomings identified’.  
   
Communication COM(2013) 847 final  
17      On the same date, 27 November 2013, the Commission adopted the communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the [European Union] (COM(2013) 847 final) (‘Communication COM(2013) 847 final’). As is clear from point 1 thereof, that communication was based inter alia on information received in the ad hoc EU-US Working Group and followed two Commission assessment reports published in 2002 and 2004 respectively.  
18      Point 1 of Communication COM(2013) 847 final explains that the functioning of Decision 2000/520 ‘relies on commitments and self-certification of adhering companies’, adding that ‘[s]igning up to these arrangements is voluntary, but the rules are binding for those who sign up’.  
19      In addition, it is apparent from point 2.2 of Communication COM(2013) 847 final that, as at 26 September 2013, 3 246 companies, falling within many industry and services sectors, were certified. Those companies mainly provided services in the EU internal market, in particular in the internet sector, and some of them were EU companies which had subsidiaries in the United States. Some of those companies processed the data of their employees in Europe which was transferred to the United States for human resource purposes.  
20      The Commission stated in point 2.2 that ‘[a]ny gap in transparency or in enforcement on the US side results in responsibility being shifted to European data protection authorities and to the companies which use the scheme’.  
21      It is apparent, in particular, from points 3 to 5 and 8 of Communication COM(2013) 847 final that, in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles.  
22      In addition, the Commission stated in point 7 of Communication COM(2013) 847 final that ‘all companies involved in the PRISM programme [a large-scale intelligence collection programme], and which grant access to US authorities to data stored and processed in the [United States], appear to be Safe Harbour certified’ and that ‘[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the [European Union]’. In that regard, the Commission noted in point 7.1 of that communication that ‘a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed [by] companies based in the [United States]’ and that ‘[t]he large-scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in [Decision 2000/520]’.  
23      In point 7.2 of Communication COM(2013) 847 final, headed ‘Limitations and redress possibilities’, the Commission noted that ‘safeguards that are provided under US law are mostly available to US citizens or legal residents’ and that, ‘[m]oreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes’.  
24      According to point 8 of Communication COM(2013) 847 final, the certified companies included ‘[w]eb companies such as Google, Facebook, Microsoft, Apple, Yahoo’, which had ‘hundreds of millions of clients in Europe’ and transferred personal data to the United States for processing.  
25      The Commission concluded in point 8 that ‘the large-scale access by intelligence agencies to data transferred to the [United States] by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the [United States]’.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
26      Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network (‘Facebook’) since 2008.  
27      Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland’s users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.   
28      On 25 June 2013 Mr Schrems made a complaint to the Commissioner by which he in essence asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency (‘the NSA’).  
29      Since the Commissioner took the view that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected it as unfounded. The Commissioner considered that there was no evidence that Mr Schrems’ personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection.  
30      Mr Schrems brought an action before the High Court challenging the decision at issue in the main proceedings. After considering the evidence adduced by the parties to the main proceedings, the High Court found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, it added that the revelations made by Edward Snowden had demonstrated a ‘significant over-reach’ on the part of the NSA and other federal agencies.  
31      According to the High Court, Union citizens have no effective right to be heard. Oversight of the intelligence services’ actions is carried out within the framework of an   
ex parte  
 and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale.  
32      The High Court stated that Irish law precludes the transfer of personal data outside national territory save where the third country ensures an adequate level of protection for privacy and fundamental rights and freedoms. The importance of the rights to privacy and to inviolability of the dwelling, which are guaranteed by the Irish Constitution, requires that any interference with those rights be proportionate and in accordance with the law.  
33      The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. In order for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards. Thus, according to the High Court, if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of a serious doubt as to whether the United States ensures an adequate level of protection of personal data, the Commissioner should have proceeded to investigate the matters raised by Mr Schrems in his complaint and that the Commissioner was wrong in rejecting the complaint.   
34      However, the High Court considers that this case concerns the implementation of EU law as referred to in Article 51 of the Charter and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter and from the principles set out by the Court of Justice in the judgment in   
Digital Rights Ireland and Others   
(C-293/12 and C-594/12, EU:C:2014:238). The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.  
35      The High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission’s finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.  
36      In those circumstances the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?  
(2)      Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?’  
   
Consideration of the questions referred  
37      By its questions, which it is appropriate to examine together, the referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.  
   
The powers of the national supervisory authorities, within the meaning of Article 28 of Directive 95/46, when the Commission has adopted a decision pursuant to Article 25(6) of that directive   
38      It should be recalled first of all that the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter (see judgments in   
Österreichischer Rundfunk and Others  
, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68;   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 68; and   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraph 29).  
39      It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms. The importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof, is, moreover, emphasised in the case-law of the Court (see judgments in   
Rijkeboer  
, C-553/07, EU:C:2009:293, paragraph 47;   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 53; and   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraphs, 53, 66, 74 and the case-law cited).  
40      As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU (see, to this effect, judgments in   
Commission  
 v   
Austria  
, C-614/10, EU:C:2012:631, paragraph 36, and   
Commission  
 v   
Hungary  
, C-288/12, EU:C:2014:237, paragraph 47).  
41      The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data (see judgments in   
Commission  
 v   
Germany  
, C-518/07, EU:C:2010:125, paragraph 25, and   
Commission  
 v   
Hungary  
, C-288/12, EU:C:2014:237, paragraph 48 and the case-law cited).  
42      In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data (see, to this effect, judgments in   
Commission   
v   
Germany  
, C-518/07, EU:C:2010:125, paragraph 24, and   
Commission  
 v   
Hungary  
, C-288/12, EU:C:2014:237, paragraph 51).  
43      The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.  
44      It is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so that they do not have powers on the basis of Article 28 in respect of processing of such data carried out in a third country.  
45      However, the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46 (see, to this effect, judgment in   
Parliament   
v   
Council and Commission  
, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines ‘processing of personal data’ as ‘any operation or set of operations which is performed upon personal data, whether or not by automatic means’ and mentions, by way of example, ‘disclosure by transmission, dissemination or otherwise making available’.  
46      Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data (see, to this effect, judgment in   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 63).  
47      As, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.  
48      Whilst acknowledging, in recital 56 in its preamble, that transfers of personal data from the Member States to third countries are necessary for the expansion of international trade, Directive 95/46 lays down as a principle, in Article 25(1), that such transfers may take place only if the third country ensures an adequate level of protection.  
49      Furthermore, recital 57 states that transfers of personal data to third countries not ensuring an adequate level of protection must be prohibited.  
50      In order to control transfers of personal data to third countries according to the level of protection accorded to it in each of those countries, Article 25 of Directive 95/46 imposes a series of obligations on the Member States and the Commission. It is apparent, in particular, from that article that the finding that a third country does or does not ensure an adequate level of protection may, as the Advocate General has observed in point 86 of his Opinion, be made either by the Member States or by the Commission.  
51      The Commission may adopt, on the basis of Article 25(6) of Directive 95/46, a decision finding that a third country ensures an adequate level of protection. In accordance with the second subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on all the Member States to which it is addressed and is therefore binding on all their organs (see, to this effect, judgments in   
Albako Margarinefabrik  
, 249/85, EU:C:1987:245, paragraph 17, and   
Mediaset  
, C-69/13, EU:C:2014:71, paragraph 23) in so far as it has the effect of authorising transfers of personal data from the Member States to the third country covered by it.   
52      Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in   
Commission  
 v   
Greece  
, C-475/01, EU:C:2004:585, paragraph 18 and the case-law cited).  
53      However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim, within the meaning of Article 28(4) of that directive, concerning the protection of their rights and freedoms in regard to the processing of that data. Likewise, as the Advocate General has observed in particular in points 61, 93 and 116 of his Opinion, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.  
54      Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities’ sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46.  
55      In particular, the first subparagraph of Article 28(4) of Directive 95/46, under which the national supervisory authorities are to hear ‘claims lodged by any person … concerning the protection of his rights and freedoms in regard to the processing of personal data’, does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive.   
56      Furthermore, it would be contrary to the system set up by Directive 95/46 and to the objective of Articles 25 and 28 thereof for a Commission decision adopted pursuant to Article 25(6) to have the effect of preventing a national supervisory authority from examining a person’s claim concerning the protection of his rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision.   
57      On the contrary, Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data. Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.   
58      If that were not so, persons whose personal data has been or could be transferred to the third country concerned would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights (see, by analogy, judgment in   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 68).  
59      A claim, within the meaning of Article 28(4) of Directive 95/46, by which a person whose personal data has been or could be transferred to a third country contends, as in the main proceedings, that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 25(6) of that directive, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.  
60      In this connection, the Court’s settled case-law should be recalled according to which the European Union is a union based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and fundamental rights (see, to this effect, judgments in   
Commission and Others  
 v   
Kadi  
, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 66;   
Inuit Tapiriit Kanatami and Others  
 v   
Parliament and Council  
, C-583/11 P, EU:C:2013:625, paragraph 91; and   
Telefónica   
v   
Commission  
, C-274/12 P, EU:C:2013:852, paragraph 56). Commission decisions adopted pursuant to Article 25(6) of Directive 95/46 cannot therefore escape such review.  
61      That said, the Court alone has jurisdiction to declare that an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, is invalid, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly (see judgments in   
Melki and Abdeli  
, C-188/10 and C-189/10, EU:C:2010:363, paragraph 54, and   
CIVAD  
, C-533/10, EU:C:2012:347, paragraph 40).   
62      Whilst the national courts are admittedly entitled to consider the validity of an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, they are not, however, endowed with the power to declare such an act invalid themselves (see, to this effect, judgments in   
Foto-Frost  
, 314/85, EU:C:1987:452, paragraphs 15 to 20, and   
IATA and ELFAA  
, C-344/04, EU:C:2006:10, paragraph 27). A fortiori, when the national supervisory authorities examine a claim, within the meaning of Article 28(4) of that directive, concerning the compatibility of a Commission decision adopted pursuant to Article 25(6) of the directive with the protection of the privacy and of the fundamental rights and freedoms of individuals, they are not entitled to declare that decision invalid themselves.  
63      Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence.  
64      In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second subparagraph of Article 28(3) of Directive 95/46, read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see, to this effect, judgment in   
T & L Sugars and Sidul Açúcares  
 v   
Commission  
, C-456/13 P, EU:C:2015:284, paragraph 48 and the case-law cited).  
65      In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, that authority must, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal proceedings. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision’s validity.  
66      Having regard to the foregoing considerations, the answer to the questions referred is that Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.  
   
The validity of Decision 2000/520  
67      As is apparent from the referring court’s explanations relating to the questions submitted, Mr Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. As the Advocate General has observed in points 123 and 124 of his Opinion, Mr Schrems expresses doubts, which the referring court indeed seems essentially to share, concerning the validity of Decision 2000/520. In such circumstances, having regard to what has been held in paragraphs 60 to 63 of the present judgment and in order to give the referring court a full answer, it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter.  
 The requirements stemming from Article 25(6) of Directive 95/46  
68      As has already been pointed out in paragraphs 48 and 49 of the present judgment, Article 25(1) of Directive 95/46 prohibits transfers of personal data to a third country not ensuring an adequate level of protection.  
69      However, for the purpose of overseeing such transfers, the first subparagraph of Article 25(6) of Directive 95/46 provides that the Commission ‘may find … that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into …, for the protection of the private lives and basic freedoms and rights of individuals’.  
70      It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country ‘shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations’ and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.  
71      However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country ‘ensures’ an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed ‘for the protection of the private lives and basic freedoms and rights of individuals’.   
72      Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.  
73      The word ‘adequate’ in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term ‘adequate level of protection’ must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.   
74      It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.  
75      Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.   
76      Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard.  
77      Moreover, as the Advocate General has stated in points 134 and 135 of his Opinion, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision’s adoption.  
78      In this regard, it must be stated that, in view of, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection, the Commission’s discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict (see, by analogy, judgment in   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 47 and 48).  
 Article 1 of Decision 2000/520  
79      The Commission found in Article 1(1) of Decision 2000/520 that the principles set out in Annex I thereto, implemented in accordance with the guidance provided by the FAQs set out in Annex II, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those principles and the FAQs were issued by the United States Department of Commerce.  
80      An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto.  
81      Whilst recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection ‘by reason of its domestic law or … international commitments’, the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice.  
82      In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are ‘intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of “adequacy” it creates’. Those principles are therefore applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them.   
83      Moreover, Decision 2000/520, pursuant to Article 2 thereof, ‘concerns only the adequacy of protection provided in the United States under the [safe harbour principles] implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive [95/46]’, without, however, containing sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments.  
84      In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, ‘to the extent necessary to meet national security, public interest, or law enforcement requirements’ and ‘by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation’.  
85      In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles’ applicability is subject, that, ‘[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law’.  
86      Thus, Decision 2000/520 lays down that ‘national security, public interest, or law enforcement requirements’ have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.  
87      In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33 and the case-law cited).  
88      In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.  
89      Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in points 204 to 206 of his Opinion, procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.  
90      Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission’s own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively, the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.  
91      As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court’s settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data (judgment in   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55 and the case-law cited).  
92      Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52 and the case-law cited).  
93      Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgment in   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).  
94      In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).   
95      Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in   
Les Verts  
 v   
Parliament  
, 294/83, EU:C:1986:166, paragraph 23;   
Johnston  
, 222/84, EU:C:1986:206, paragraphs 18 and 19;   
Heylens and Others  
, 222/86, EU:C:1987:442, paragraph 14; and   
UGT-Rioja and Others  
, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80).  
96      As has been found in particular in paragraphs 71, 73 and 74 of the present judgment, in order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment.  
97      However, the Commission did not state, in Decision 2000/520, that the United States in fact ‘ensures’ an adequate level of protection by reason of its domestic law or its international commitments.  
98      Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.  
 Article 3 of Decision 2000/520  
99      It is apparent from the considerations set out in paragraphs 53, 57 and 63 of the present judgment that, under Article 28 of Directive 95/46, read in the light in particular of Article 8 of the Charter, the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person’s rights and freedoms in regard to the processing of personal data relating to him. That is in particular the case where, in bringing such a claim, that person raises questions regarding the compatibility of a Commission decision adopted pursuant to Article 25(6) of that directive with the protection of the privacy and of the fundamental rights and freedoms of individuals.   
100    However, the first subparagraph of Article 3(1) of Decision 2000/520 lays down specific rules regarding the powers available to the national supervisory authorities in the light of a Commission finding relating to an adequate level of protection, within the meaning of Article 25 of Directive 95/46.  
101    Under that provision, the national supervisory authorities may, ‘[w]ithout prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive [95/46], … suspend data flows to an organisation that has self-certified its adherence to the [principles of Decision 2000/520]’, under restrictive conditions establishing a high threshold for intervention. Whilst that provision is without prejudice to the powers of those authorities to take action to ensure compliance with national provisions adopted pursuant to Directive 95/46, it excludes, on the other hand, the possibility of them taking action to ensure compliance with Article 25 of that directive.  
102    The first subparagraph of Article 3(1) of Decision 2000/520 must therefore be understood as denying the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.  
103    The implementing power granted by the EU legislature to the Commission in Article 25(6) of Directive 95/46 does not confer upon it competence to restrict the national supervisory authorities’ powers referred to in the previous paragraph of the present judgment.  
104    That being so, it must be held that, in adopting Article 3 of Decision 2000/520, the Commission exceeded the power which is conferred upon it in Article 25(6) of Directive 95/46, read in the light of the Charter, and that Article 3 of the decision is therefore invalid.  
105    As Articles 1 and 3 of Decision 2000/520 are inseparable from Articles 2 and 4 of that decision and the annexes thereto, their invalidity affects the validity of the decision in its entirety.  
106    Having regard to all the foregoing considerations, it is to be concluded that Decision 2000/520 is invalid.  
   
Costs  
107    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.  
2.        
Decision 2000/520 is invalid.

ID: 543e4b1b-8d86-4711-b378-ad4b4d4a19a8

Judgment of 1 Oct 2015, C-201/14 (  
Bara and Others  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Information to be provided in case of direct collection   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
 Information to be provided in case of indirect collection   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness, fairness and transparency   
   
JUDGMENT OF THE COURT (Third Chamber)  
1 October 2015 (\*)  
(Reference for a preliminary ruling — Directive 95/46/EC — Processing of personal data — Articles 10 and 11 — Data subjects’ information — Article 13 — Exceptions and limitations — Transfer by a public administrative body of a Member State of personal tax data for processing by another public administrative body)  
In Case C-201/14,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Curtea de Apel Cluj (Romania), made by decision of 31 March 2014, received at the Court on 22 April 2014, in the proceedings  
Smaranda Bara and Others  
v  
Președintele Casei Naționale de Asigurări de Sănătate,  
Casa Naţională de Asigurări de Sănătate,  
Agenţia Naţională de Administrare Fiscală (ANAF),  
THE COURT (Third Chamber),  
composed of M. Ilešič, President of the Chamber, A. Ó Caoimh, C. Toader, E. Jarašiūnas and C.G. Fernlund (Rapporteur), Judges,  
Advocate General: P. Cruz Villalón,  
Registrar: L. Carrasco Marco, Administrator,  
having regard to the written procedure and further to the hearing on 29 April 2015,  
after considering the observations submitted on behalf of:  
–        Smaranda Bara and Others, by C.F. Costaş and M.K. Kapcza, avocați,  
–        the Casa Naţională de Asigurări de Sănătate, by V. Ciurchea, acting as Agent,  
–        the Romanian Government, by R.H. Radu and by A. Buzoianu, A.-G. Văcaru and D.M. Bulancea, acting as Agents,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the European Commission, by I. Rogalski and B. Martenczuk and by J. Vondung, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 9 July 2015,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 124 TFEU and Articles 10, 11 and 13 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p.31).  
2        The request has been made in proceedings between, on the one hand, Smaranda Bara and others, the applicants in the main proceedings, and, on the other hand, the Președintele Casei Naționale de Asigurări de Sănătate (Director of the National Health Insurance Fund), the Casa Naționale de Asigurări de Sănătate (the National Health Insurance Fund, ‘the CNAS’), and the Agenția Națională de Administrare Fiscală (National Tax Administration Agency, ‘the ANAF’) concerning the processing of certain data.  
   
Legal context  
   
EU law  
3        Article 2 of Directive 95/46, headed ‘Definitions’, provides:   
‘For the purpose of this Directive:   
(a)       “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)       “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
(c)      “personal data filing system” (“filing system”) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;  
…’  
4        Article 3 of that directive, entitled ‘Scope’, is worded as follows:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
5        Article 6 of that directive, which concerns the principles relating to data quality, provides:  
‘1.       Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
6        Article 7 of that directive, which concerns the criteria for making data processing legitimate, states:   
‘Member States shall provide that personal data may be processed only if:   
(a)      the data subject has unambiguously given his consent; or   
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or   
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject; or  
(d)      processing is necessary in order to protect the vital interests of the data subject; or   
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
7        Article 10 of Directive 95/46, entitled ‘Information in cases of collection of data from the data subject’, provides:  
‘Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:  
(a)      the identity of the controller and of his representative, if any;   
(b)      the purposes of the processing for which the data are intended;  
(c)      any further information such as:  
–        the recipients or categories of recipients of the data,  
–        whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,  
–        the existence of the right of access to and the right to rectify the data concerning him  
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.’  
8        Article 11 of the directive, entitled ‘Information where the data have not been obtained from the data subject’, is worded as follows:  
‘1.      Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:  
(a)      the identity of the controller and of his representative, if any;  
(b)      the purposes of the processing;  
(c)      any further information such as:  
–        the categories of data concerned,  
–        the recipients or categories of recipients,  
–        the existence of the right of access to and the right to rectify the data concerning him  
in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.  
2.      Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.’  
9        Under Article 13 of the directive, entitled ‘Exemptions and restrictions’:  
‘1.      Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:  
(a)       national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
(e)      an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;  
(f)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);  
(g)       the protection of the data subject or of the rights and freedoms of others.  
2.       Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.’  
   
Romanian law  
 Law No 95/2006  
10      It is apparent from the order for reference, Article 215 of Law No 95/2006 concerning reform in the field of health (Legea nr. 95/2006 privind reforma în domeniul sănătății), of 14 April 2006 (  
Monitorul Oficial al României  
, Part I, No 372 of 28 April 2006), provides:  
‘(1)      the requirement to pay health insurance contributions is incumbent on any natural or legal person who engages persons under an individual contract of employment or by virtue of special rules provided for by statute and, as the case may be, on natural persons.  
(2)      The natural or legal persons for whom the insured persons carry out their activities shall be required to submit on a monthly basis to the health insurance fund freely chosen by the insured person statements, identifying the insured persons by name, as to the natural or legal person’s obligations to the fund and proof that contributions have been paid.  
…’  
11      Article 315 of that law states:   
‘the data necessary to certify that the person concerned qualifies as an insured person are to be communicated free of charge to the health insurance funds by the authorities, public institutions or other institutions in accordance with a protocol.’  
 Order No 617/2007 of the Director of the CNAS  
12      Article 35 of Order No 617/2007 of the Director of the CNAS, of 13 August 2007, approving the implementing measures relating to identifying documentary evidence required for the purpose of qualifying as an insured person, or an insured person who is not required to make contributions, and applying measures for the recovery of sums owing to the Joint National Health Insurance Fund (  
Monitorul Oficial al României  
, Part I, No 649 of 24 September 2007), provides:  
‘[…] with regard to the requirement to make payments to the fund on the part of natural persons who obtain insurance cover by means of insurance contracts, other than such persons from whom tax is collected by the ANAF, the following shall constitute evidence of liability, depending on the circumstances: the declaration …, in the notification of tax liability issued by the competent body of the CAS [Health Insurance Fund] and judicial decisions concerning sums owing to the fund. The notification of tax liability may be issued by the competent body of the CAS also on the basis of information received from the ANAF in accordance with a protocol.’  
 The 2007 Protocol  
13      Article 4 of Protocol No P 5282/26.10.2007/95896/30.10.2007 concluded between the CNAS and the ANAF (‘the 2007 Protocol’), provides:  
‘after the entry into force of this Protocol, the [ANAF] shall provide in electronic format, by means of its specialised supporting units, the original database concerning:  
a.       the income of persons forming part of the categories identified in Article 1(1) of this Protocol and, on a three-monthly basis, the updated version of that database, to the [CNAS], in a form compatible with automated processing, in accordance with Annex I to this Protocol …  
…’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
14      The applicants in the main proceedings earn income from self-employment. The ANAF transferred data relating to their declared income to the CNAS. On the basis of that data, the CNAS required the payment of arrears of contributions to the health insurance regime.  
15      The applicants in the main proceedings brought an appeal before the Curtea de Apel Cluj (Court of Appeal, Cluj), in which they challenged the lawfulness of the transfer of tax data relating to their income in the light of Directive 95/46. They submit that the personal data were, on the basis of a single internal protocol, transferred and used for purposes other than those for which it had initially been communicated to the ANAF, without their prior explicit consent and without their having previously been informed.  
16      According to the order for reference, public bodies are empowered, under Law No 95/2006, to transfer personal data to the health insurance funds so that the latter may determine whether an individual qualifies as an insured person. The data concern the identification of persons (surname, first name, personal identity card number, address) but does not include data relating to income received.   
17      The referring court wishes to determine whether the processing of the data by the CNAS required prior information to be given to the data subjects as to the identity of the data controller and the purpose for which the data was transferred. That court is also asked to determine whether the transfer of the data on the basis of the 2007 Protocol is contrary to Directive 95/46 which requires that all restrictions on the rights of data subjects are laid down by law and accompanied by safeguards, in particular when the data is used against those persons.   
18      In those circumstances, the Curtea de Apel Cluj decided to stay proceedings and refer the following questions to the Court for a preliminary ruling:  
‘(1)      Is a national tax authority, as the body representing the competent ministry of a Member State, a financial institution within the meaning of Article 124 TFEU?  
(2)      Is it possible to make provision, by means of a measure akin to an administrative measure, namely a protocol concluded between the national tax authority and another State institution, for the transfer of the database relating to the income earned by the citizens of a Member State from the national tax authority to another institution of the Member State, without giving rise to a measure establishing privileged access, as defined in Article 124 TFEU?   
(3)      Is the transfer of the database, the purpose of which is to impose an obligation on the citizens of the Member State to pay social security contributions to the Member State institution for whose benefit the transfer is made, covered by the concept of prudential considerations within the meaning of Article 124 TFEU?  
(4)      May personal data be processed by authorities for which such data were not intended where such an operation gives rise, retroactively, to financial loss?’  
   
The questions referred  
   
Admissibility  
 Admissibility of the first to third questions  
19      According to settled case-law, the Court may refuse to rule on a question referred for a preliminary ruling by a national court where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its object, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see judgment in   
PreussenElektra  
, C-379/98, EU:C:2001:160, paragraph 39 and the case-law cited).   
20      All of the observations presented to the Court submit that the first to third questions referred concerning the interpretation of Article 124 TFEU are inadmissible on the ground that they bear no relation to the object of the dispute in the main proceedings.   
21      In that regard, it must be recalled that Article 124 TFEU falls within Part Three of the TFEU, under Title VIII on economic and monetary policy. That article prohibits any measure, not based on prudential considerations, establishing privileged access by Union institutions, bodies, offices or agencies, central governments, regional, local or other public authorities, other bodies governed by public law, or public undertakings of Member States to financial institutions.  
22      The origin of that prohibition is to be found in Article 104 A of the EC Treaty (which became Article 102 EC), which was inserted in the EC Treaty by the Treaty of Maastricht. It was one of the provisions of the TFEU relating to the economic policy that intended to encourage the Member States to follow a sound budgetary policy, not allowing monetary financing of public deficits or privileged access by public authorities to the financial markets to lead to excessively high levels of debt or excessive Member State deficits (see, to that effect, judgment in   
Gauweiler and Others  
, C-62/14, EU:C:2015:400, paragraph 100).  
23      It is, therefore, quite obvious that the interpretation of Article 124 TFEU requested bears no relation to the actual facts or object of the dispute in the main proceedings, which concerns the protection of personal data.   
24      It follows that it is not necessary to reply to the first to third questions.  
 Admissibility of the fourth question  
25      The CNAS and the Romanian Government submit that the fourth question is inadmissible. That government submits that there is no link between the damage relied on by the applicants in the main proceedings and the annulment of the administrative acts contested within those proceedings.   
26      In that regard, it must be borne in mind that, according to the settled case-law of the Court, questions on the interpretation of EU law referred by a national court in the factual and legislative context which that court is responsible for defining, the accuracy of which is not a matter for the Court to determine, enjoy a presumption of relevance. The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment in   
Fish Legal and Shirley  
, C-279/12, EU:C:2013:853, paragraph 30 and the case-law cited).   
27      It must be observed that the main proceedings concern the lawfulness of processing of tax data collected by the ANAF. The referring court is uncertain as to the interpretation of Directive 95/46, in the context of reviewing the lawfulness of the transfer of those data to the CNAS and their subsequent processing. The fourth question referred is therefore relevant and sufficiently precise to enable the Court to give a useful answer. Accordingly, the request for a preliminary ruling must be held to be admissible as regards the fourth question.   
   
Substance  
28      By its fourth question, the referring court asks, in essence, whether Articles 10, 11 and 13 of Directive 95/46 must be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow a public administrative body in a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects being informed of that transfer and processing.  
29      In that regard, it must be held, on the basis of the information provided by the referring court, that the tax data transferred to the CNAS by the ANAF are personal data within the meaning of Article 2(a) of the directive, since they are ‘information relating to an identified or identifiable natural person’ (judgment in   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 35). Both the transfer of the data by the ANAF, the body responsible for the management of the database in which they are held, and their subsequent processing by the CNAS therefore constitute ‘processing of personal data’ within the meaning of Article 2(b) of the directive (see, to that effect, inter alia, judgments in   
Österreichischer Rundfunk and Others  
, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 64, and   
Huber  
, C-524/06, EU:C:2008:724, paragraph 43).   
30      In accordance with the provisions of Chapter II of Directive 95/46, entitled ‘General rules on the lawfulness of the processing of personal data’, subject to the exceptions permitted under Article 13 of that directive, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (judgments in   
Österreichischer Rundfunk and Others  
, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 65;   
Huber  
, C-524/06, EU:C:2008:724, paragraph 48; and   
ASNEF and FECEMD  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 26).  
31      Furthermore, the data controller or his representative is obliged to provide information in accordance with the requirements laid down in Articles 10 and 11 of Directive 95/46, which vary depending on what data are, or are not, collected from the data subject, and subject to the exceptions permitted under Article 13 of the directive.  
32      As regards, first, Article 10 of the directive, that article provides that the data controller must provide a data subject, from whom data relating to himself are collected, with the information listed in subparagraphs (a) to (c), except where he already has that information. That information concerns the identity of the data controller, the purposes of the processing and any further information necessary to guarantee fair processing of the data. Amongst the additional information necessary to guarantee fair processing of the data, Article 10(c) of the directive expressly refers to ‘recipients or categories of recipients of the data’ and ‘the existence of a right of access to and the right to rectify the data concerning [that person]’.  
33      As the Advocate General observed in point 74 of his Opinion, the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, set out in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive.   
34      It follows that the requirement of fair processing of personal data laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of those data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data.  
35      It is clear from the information provided by the referring court that the applicants in the main proceedings were not informed by the ANAF of the transfer to the CNAS of personal data relating to them.  
36      The Romanian Government submits, however, that the ANAF is required, in particular under Article 315 of Law No 95/2006, to transfer to the regional health insurance funds the information necessary for the determination by the CNAS as to whether persons earning income through self-employment qualify as insured persons.  
37      It is true that Article 315 of Law No 95/2006 expressly provides that ‘the data necessary to certify that the person concerned qualifies as an insured person are to be communicated free of charge to the health insurance funds by the authorities, public institutions or other institutions in accordance with a protocol’. However, it is clear from the explanations provided by the referring court that the data necessary for determining whether a person qualifies as an insured person, within the meaning of the abovementioned provision, do not include those relating to income, since the law also recognises persons without a taxable income as qualifying as insured.  
38      In those circumstances, Article 315 of Law No 95/2006 cannot constitute, within the meaning of Article 10 of Directive 95/46, prior information enabling the data controller to dispense with his obligation to inform the persons from whom data relating to their income are collected as to the recipients of those data. Therefore, it cannot be held that the transfer at issue was carried out in compliance with Article 10 of Directive 95/46.  
39      It is necessary to examine whether Article 13 of the directive applies to that failure to inform the data subjects. It is apparent from Article 13(1)(e) and (f) that Member States may restrict the scope of the obligations and rights provided for in Article 10 of the same directive when such a restriction constitutes a necessary measure to safeguard ‘an important economic or financial interest of a Member State […], including monetary, budgetary and taxation matters’ or ‘a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e)’. Nevertheless, Article 13 expressly requires that such restrictions are imposed by legislative measures.  
40      Apart from the fact, noted by the referring court, that data relating to income are not part of the personal data necessary for the determination of whether a person is insured, it must be observed that Article 315 of Law No 95/2006 merely envisages the principle of the transfer of personal data relating to income held by authorities, public institutions and other institutions. It is also apparent from the order for reference that the definition of transferable information and the detailed arrangements for transferring that information were laid down not in a legislative measure but in the 2007 Protocol agreed between the ANAF and the CNAS, which was not the subject of an official publication.   
41      In those circumstances, it cannot be concluded that the conditions laid down in Article 13 of Directive 95/46 permitting a Member State to derogate from the rights and obligations flowing from Article 10 of the directive are complied with.   
42      As regards, in the second place, Article 11 of the directive, paragraph 1 of that article provides that a controller of data which were not obtained from the data subject must provide the latter with the information listed in subparagraphs (a) to (c). That information concerns the identity of the data controller, the purposes of the processing, and any further information necessary to ensure the fair processing of the data. Amongst that further information, Article 11(1)(c) of the directive refers expressly to ‘the categories of data concerned’ and ‘the existence of the right of access to and the right to rectify the data concerning him’.  
43      It follows that, in accordance with Article 11(1)(b) and (c) of Directive 95/46, in the circumstances of the case in the main proceedings, the processing by the CNAS of the data transferred by the ANAF required that the subjects of the data be informed of the purposes of that processing and the categories of data concerned.   
44      It is apparent from the information given by the referring court, however, that the CNAS did not provide the applicants in the main proceedings with the information listed in Article 11(1)(a) to (c) of the directive.   
45      It is appropriate to add that, in accordance with Article 11(2) of Directive 95/46, the provisions of Article 11(1) of the directive do not apply when, in particular, the registration or communication of the data are laid down by law, Member States being required to provide appropriate safeguards in those cases. For the reasons set out in paragraphs 40 and 41 of this judgment, the provisions of Law No 95/2006 relied on by the Romanian Government and the 2007 Protocol do not establish a basis for applying either the derogation under Article 11(2) or that provided for under Article 13 of the directive.   
46      Having regard to all the foregoing considerations, the answer to the question referred is that Articles 10, 11 and 13 of Directive 95/46 must be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow a public administrative body of a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects having been informed of that transfer or processing.   
   
Costs  
47      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Articles 10, 11 and 13 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, must be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow a public administrative body of a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects having been informed of that transfer or processing.

ID: 557d63f9-d37f-4821-ad63-b81949fcd0ed

Judgment of 15 Mar 2017, C-536/15 (  
Tele2 (Netherlands)  
)  
E-privacy Directive   
 >   
Electronic communications   
 >   
Directories of subscribers   
   
JUDGMENT OF THE COURT (Second Chamber)  
15 March 2017 (\*)  
(Reference for a preliminary ruling — Electronic communications networks and services — Directive 2002/22/EC — Article 25(2) — Directory enquiry services and directories — Directive 2002/58/EC — Article 12 — Directories of subscribers — Making available personal data concerning subscribers for the purposes of the provision of publicly available directory enquiry services and directories — Subscriber’s consent — Distinction on the basis of the Member State in which publicly available directory enquiry services and directories are provided — Principle of non-discrimination)  
In Case C-536/15,  
REQUEST for a preliminary ruling under Article 267 TFEU from the College van Beroep voor het bedrijfsleven (Administrative Court of Appeal for Trade and Industry, Netherlands), made by decision of 3 July 2015, received at the Court on 13 October 2015, in the proceedings  
Tele2 (Netherlands) BV,  
Ziggo BV,  
Vodafone Libertel BV  
v  
Autoriteit Consument en Markt (ACM),  
intervening parties:  
European Directory Assistance NV,  
THE COURT (Second Chamber),  
composed of M. Ilešič, President of the Chamber, A. Prechal, A. Rosas, C. Toader and E. Jarašiūnas (Rapporteur), Judges,  
Advocate General: M. Y. Bot,  
Registrar: M. R. Schiano, Administrator,  
having regard to the written procedure and further to the hearing on 5 October 2016,  
after considering the observations submitted on behalf of:  
–        Tele2 (Netherlands) BV, by Q.R. Kroes and M.P.F. Reker, advocaten,  
–        Ziggo BV, by W. Knibbeler and N. Lorjé, advocaten,  
–        Vodafone Libertel BV, by H.P. Wiersema, advocaat,  
–        the Netherlands Government, by M. de Ree and M. Bulterman and by J. Langer, acting as Agents,  
–        the European Commission, by H. Kranenborg and G. Braun and by L. Nicolae, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 9 November 2016,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 25(2) of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users’ rights relating to electronic communications networks and services (Universal Service Directive) (OJ 2002 L 108, p. 51), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘the Universal Service Directive’).  
2        The request has been made in proceedings between Tele2 (Netherlands) BV, Ziggo BV and Vodafone Libertel BV, companies established in the Netherlands, on the one hand, and the Autoriteit Consument en Markt (ACM) (Authority for Consumers and Markets), on the other hand, concerning a decision taken by that authority in the context of proceedings between those undertakings and the European Directory Assistance NV (‘the EDA’), an undertaking established in another Member State, concerning the latter making data relating to their subscribers available, for the purposes of the provision of publicly available directory enquiry services and directories in the latter Member State and/or in other Member States.  
   
Legal context  
   
European Union law  
   
The Universal Service Directive  
3        Recitals 11 and 35 of the Universal Service Directive states:  
‘(11) … Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [(OJ 1998 L 24, p. 1)] ensures the subscribers’ right to privacy with regard to the inclusion of their personal information in a public directory.  
…  
(35)      The provision of directory enquiry services and directories is already open to competition. The provisions of this Directive complement the provisions of Directive 97/66/EC by giving subscribers a right to have their personal data included in a printed or electronic directory. All service providers which assign telephone numbers to their subscribers are obliged to make relevant information available in a fair, cost-oriented and non-discriminatory manner.’  
4        Article 1 of that directive, entitled ‘Subject-matter and scope’, provides in paragraph (1):  
‘Within the framework of Directive 2002/21/EC [of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ 2002 L 108, p. 33)], this Directive concerns the provision of electronic communications networks and services to end-users. The aim is to ensure the availability throughout the [European Union] of good-quality publicly available services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market. …’  
5        Chapter II of the Universal Service Directive concerns universal service obligations. In that chapter, Article 5, entitled ‘Directory enquiry services and directories’, is worded as follows:  
‘(1)      Member States shall ensure that:  
(a)      at least one comprehensive directory is available to end-users in a form approved by the relevant authority, whether printed or electronic, or both, and is updated on a regular basis, and at least once a year;  
(b)      at least one comprehensive telephone directory enquiry service is available to all end-users, including users of public pay telephones.  
(2)      The directories referred to in paragraph 1 shall comprise, subject to the provisions of Article 12 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [(OJ 2002 L 201, p. 37)], all subscribers of publicly available telephone services.  
…’  
6        Chapter IV of the Universal Service Directive concerns end-user interests and rights. In that chapter, Article 25, entitled ‘Telephone directory enquiry services’, provides:  
‘(1)      Member States shall ensure that subscribers to publicly available telephone services have the right to have an entry in the publicly available directory referred to in Article 5(1)(a) and to have their information made available to providers of directory enquiry services and/or directories in accordance with paragraph 2’;  
(2)      Member States shall ensure that all undertakings which assign telephone numbers to subscribers meet all reasonable requests to make available, for the purposes of the provision of publicly available directory enquiry services and directories, the relevant information in an agreed format on terms which are fair, objective, cost oriented and non-discriminatory.  
…  
(5)      Paragraphs 1 to 4 shall apply subject to the requirements of [Union] legislation on the protection of personal data and privacy and, in particular, Article 12 of Directive 2002/58 …’  
   
The Directive on privacy and electronic communications  
7        According to recital 39 of Directive 2002/58, as amended by Directive 2009/136 (‘the Directive on privacy and electronic communications’):  
‘(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.’  
8        Article 1 of the Directive on privacy and electronic communications, entitled ‘Scope and aim’, provides in paragraph (1):  
‘This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the [Union].’  
9        Article 12 of that directive, entitled ‘Directories of subscribers’, provides:  
‘(1)      Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.  
(2)      Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.  
(3)      Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.  
…’  
   
Netherlands law  
10      Under Article 1.1(e) of the Besluit universele dienstverlening en eindgebruikersbelangen (Decree on universal service provision and end-user interests) of 7 May 2004 (Stb. 2004, No 203) (‘the Bude’):  
‘A standard directory enquiry service means a publicly available directory enquiry service by means of which telephone numbers can be requested only on the basis of data relating to the name in conjunction with data relating to the address and house number, post code or town of the subscriber.’  
11      Article 3.1 of the Bude is worded as follows:  
‘Any provider which assigns telephone numbers shall meet all reasonable requests to make available, for the purposes of the provision of publicly available telephone directories and publicly available directory enquiry services, the relevant information in an agreed format on terms which are fair, objective, cost oriented and non-discriminatory.’  
12      Under Article 3.2 of the Bude:  
‘(1)      Any provider of a publicly available telephone service which, before or when concluding a contract with a user, requests the latter’s name and address (street name and house number, post code and town), shall also seek his consent to that kind of personal data and the telephone numbers it has assigned appearing in any standard telephone directory and any directory of subscribers which is used for a standard directory enquiry service. The consent referred to in the preceding sentence shall be sought individually for every kind of personal data.  
(2)      The consent given shall constitute relevant information within the meaning of Article 3.1.  
(3)      Any provider of a publicly available telephone service which also seeks consent for inclusion in a telephone directory other than the standard telephone directory or in a directory of subscribers not exclusively used for a standard directory enquiry service shall ensure that the manner and form in which the consent referred to in paragraph 1 is sought is at least equivalent to the manner and form in which the original consent referred to in this paragraph is sought.’  
13      Article 11.6 of the Telecommunicatiewet (Telecommunications Law) of 19 October 1998 (Stb. 1998, No 610) provides:  
‘(1)      Any person who publishes a publicly available directory or who supplies information services about subscribers available to the public shall, prior to entering private data relating to subscribers in the directory or in the directory of subscribers used for a standard directory enquiry service, provide information free of charge to subscribers concerning:  
(a)      the purposes for which the directories and directory enquiry services at issue which concern subscribers are established and, with regard to electronic versions of the directory, the possibilities for use to be made of that information on the basis of search functions integrated into those versions, and  
(b)      the types of personal data which can be included in the directories and directory enquiry services at issue which concern subscribers, in the light of the purposes for which they are established.  
(2)      A directory available to the public and the directory of subscribers used for directory enquiry services shall reproduce the personal data of a subscriber only if the latter has given his consent and shall be limited to data provided for that purpose by the subscriber. No fee shall be charged for not being included in a directory or in a directory of subscribers used for directory enquiry services.  
(3)      In so far as the processing of personal data included in a publicly available directory and in a directory of subscribers used for directory enquiry services pursues objectives other than the possibility of making a search for numbers in a database relating to a name associated with data such as the road, house number, postal code and town of the subscriber, the subscriber’s separate consent is required for each of those other objectives.  
(4)      The subscriber shall have the right to verify, correct and delete, free of charge, the personal data relating to him in a publicly available directive or in a directory of subscribers used for directory enquiry services.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
14      EDA is a company incorporated under Belgian law which offers directory enquiry services and directories accessible from Belgian territory. It requested the undertakings which assign telephone numbers to subscribers in the Netherlands (‘the Dutch undertakings’) to make available to it data relating to their subscribers. Since those undertakings refused to provide the data requested, on 18 January 2012, EDA submitted a dispute resolution request to ACM.  
15      By decisions of 5 June 2013, ACM, as the national regulatory authority, took a decision on EDA’s request by adopting the following measures. First, EDA can rely on Article 3.1 of the Bude to the extent that it uses the numbers made available to it and the related information in order to place a standard telephone directory enquiry service about the subscribers on the market. Secondly, the Dutch undertakings must make available to EDA basic data relating to their subscribers (names, addresses, telephone numbers) on fair, objective, cost oriented and non-discriminatory terms. Third, the Dutch undertakings must ensure within a reasonable period of time that the consent which they seek from their subscribers when entering into contracts, with a view to including the data concerning them in any standard directory and any directory of subscribers which is used for a standard telephone directory enquiry service is compatible with the provisions of Article 3.2 of the Bude.  
16      The Dutch undertakings brought an action against those decisions of ACM before the College van Beroep voor het bedrijfsleven (Administrative Court of Appeal for Trade and Industry, Netherlands).  
17      The referring court states, in the first place, that, given that Article 3.1 of the Bude transposed into Netherlands law Article 25(2) of the Universal Service Directive, it is necessary to establish the scope of the latter provision in order to answer the question, which is disputed by the parties to the main proceedings, whether that Article 3.1 requires Dutch undertakings to make available to EDA data relating to their subscribers despite the fact that EDA is not established in the Netherlands.  
18      It notes, in that regard, that the interpretation of Article 25(2) of that directive given by the Court in the judgment of 5 May 2011,   
Deutsche Telekom   
(C-543/09, EU:C:2011:279), does not involve the cross-border provision of data relating to subscribers and does not, consequently, answer the question whether that provision must be interpreted as meaning that an undertaking is required to make its data relating to subscribers available to a provider of directory enquiry services and directories established in another Member State.  
19      In the second place, the referring court notes, concerning obtaining the subscriber’s consent, that Article 3.2 of the Bude provides that the provider is to obtain that consent to the inclusion of personal data and telephone numbers use of which it has assigned, in any standard directory and any directory of subscribers which is used for a standard telephone directory enquiry service. It points out that, according to the explanatory notes to Article 3.2 of the Bude, ‘the reason for that is to avoid a situation where every provider of publicly available telephone directories and directory enquiry services would have to obtain the consent of every subscriber individually for a standard listing’.  
20      The referring court notes that the parties to the main proceedings dispute whether, first, Article 3.2 of the Bude allows the consent of subscribers to the use of their personal data to be differentiated according to whether those data are intended for Dutch providers or for foreign providers of directory enquiry services and/or directories and, secondly, whether it is necessary to leave the subscribers with the choice whether or not to give their consent depending on the country in which the undertaking requesting information provides its services. In that regard, the referring court considers that the question arises, in essence, as to how to balance respect for the principle of non-discrimination and privacy in the context of that request for consent.  
21      In those circumstances, the College van Beroep voor het bedrijfsleven (Administrative Court of Appeal for Trade and Industry) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must Article 25(2) of the Universal Service Directive be interpreted as meaning that requests should be understood to include a request from an undertaking established in another Member State, which requests information for the purposes of the provision of publicly available telephone directory enquiry services and directories which are provided in that Member State and/or in other Member States?  
(2)      If question 1 is answered in the affirmative: may a provider who makes telephone numbers available, and who is obliged under national legislation to request a subscriber’s consent prior to inclusion [of his data] in standard telephone directories and standard directory enquiry services, differentiate in the request for consent on the basis of the non-discrimination principle according to the Member State in which the undertaking requesting the information as referred to in Article 25(2) of Directive 2002/22/EC provides the telephone directory and directory enquiry service?’  
   
Consideration of the questions referred  
   
The first question  
22      By its first question, the referring court asks, in essence, whether Article 25(2) of the Universal Service Directive must be interpreted as meaning that the concept of ‘requests’, in that article, covers also requests made by an undertaking, established in a Member State other than that in which the undertakings which assign telephone numbers to subscribers are established, which requests the relevant information possessed by those undertakings in order to provide publicly available telephone directory enquiry services and directories in that Member State and/or in other Member States.  
23      Article 25 of the Universal Service Directive is in Chapter IV of that directive, which concerns end-user interests and rights. According to Article 25(1) thereof, the Member States are to ensure that subscribers to publicly available telephone services have the right to have an entry in the publicly available directory referred to in Article 5(1)(a) of that directive, and to have their information made available to providers of directory enquiry services and/or directories in accordance with Article 25(2) of that directive.  
24      Concerning the making of information relating to subscribers available to providers of directory services and/or directories, it is apparent from the wording itself of Article 25(2) of the Universal Service Directive that that provision covers all reasonable requests to make available data for the purposes of the provision of publicly available directory enquiry services and directories. Moreover, that provision requires that that information be made available in a non-discriminatory manner.  
25      It follows therefore from that wording that that provision makes no distinction according to whether the request to make available data relating to subscribers is made by an undertaking established in the same Member State as that in which is established the undertaking to which the request is addressed or whether it is made by an undertaking established in a Member State other than that of the undertaking which received that request.  
26      That lack of distinction is compatible with the objective pursued by the Universal Service Directive, which, according to Article 1(1) thereof, seeks, in particular, to ensure the availability, throughout the European Union, of good quality publicly available services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market, and with the specific objective of Article 25(2) of the Universal Service Directive which seeks, in particular, to ensure compliance with the universal service obligation laid down in Article 5(1) of that directive (see, to that effect, judgment of 5 May 2011,   
Deutsche Telekom  
, C-543/09, EU:C:2011:279, paragraph 35).  
27      In that regard, the Court has already held, in paragraph 36 of the judgment of 5 May 2011,   
Deutsche Telekom  
 (C-543/09, EU:C:2011:279), referring to recital 35 of the Universal Service Directive, that, in a competitive market, the obligation under Article 25(2) of that directive for undertakings which assign telephone numbers to pass on data relating to their own subscribers in principle not only enables the designated undertaking to ensure compliance with the universal service obligation laid down in Article 5(1) of that directive, but also enables any provider of telephone services to establish an exhaustive data base and to become active in the market for telephone directory enquiry services and directories. In that connection, it is sufficient that the provider concerned ask each undertaking assigning telephone numbers for the relevant data relating to its subscribers.  
28      An interpretation of Article 25(2) of the Universal Service Directive according to which that provision covers only reasonable requests made by undertakings established in the Member State in which the undertakings assigning telephone numbers to subscribers are established would be contrary to the objective of ensuring the availability, throughout the European Union, of good quality services to end-users thanks to effective competition and, in particular, to that of respecting the universal service obligation provided for in Article 5(1) of the Universal Service Directive, resulting, in particular, from the need to make at least one complete telephone directory available to end-users.  
29      Moreover, as was stated in paragraph 24 of the present judgment, Article 25(2) of the Universal Service Directive requires undertakings assigning telephone numbers to subscribers to meet all reasonable requests to make available, for the purposes of the provision of publicly available directory enquiry services and directories, the relevant information in a non-discriminatory manner. The refusal of undertakings assigning telephone numbers to subscribers in the Netherlands to make data relating to their subscribers available to persons requesting that information on the sole ground that they are established in another Member State is incompatible with that requirement.  
30      In the light of all the above considerations, the answer to the first question is that Article 25(2) of the Universal Service Directive must be interpreted as meaning that the concept of ‘requests’ in that article, covers also requests made by an undertaking, established in a Member State other than that in which the undertakings which assign telephone numbers to subscribers are established, which requests the relevant information possessed by those undertakings in order to provide publicly available telephone directory enquiry services and directories in that Member State and/or in other Member States.  
   
The second question  
31      By its second question, the referring court asks, in essence, whether Article 25(2) of the Universal Service Directive must be interpreted as precluding an undertaking which assigns telephone numbers to subscribers, and which is obliged under national legislation to request those subscribers’ consent to the use of data relating to them for the purposes of supplying directory enquiry services and directories, from differentiating in the request for those subscribers’ consent to that use according to the Member State in which the undertakings requesting the information referred to in that provision provide those services.  
32      Under Article 25(2) of the Universal Service Directive, the Member States are to ensure that all undertakings which assign telephone numbers to subscribers meet all reasonable requests for information to be made available, for the purposes of the provision of telephone directory enquiry services and telephone directories, on terms that must be fair, objective, cost oriented and non-discriminatory. Moreover, it is apparent from Article 25(5) of that directive that Article 25(2) thereof is to apply ‘subject to the requirements of Union legislation on the protection of personal data and privacy and, in particular, Article 12 of [the Directive on privacy and electronic communications]’.  
33      It follows that, in order to answer the second question, it is necessary to examine also whether Article 12(2) of that directive subjects the transfer, by an undertaking which assigns telephone numbers to its subscribers, of a subscriber’s personal data to a third-party undertaking whose activity consists in providing publicly available directory enquiry services and directories in a Member State other than that in which that subscriber resides, to the latter’s separate specific consent.  
34      In that regard, it should be noted that the Court held, in paragraph 67 of the judgment of 5 May 2011,   
Deutsche Telekom  
 (C-543/09, EU:C:2011:279), that Article 12 of that directive must be interpreted as not precluding national legislation under which an undertaking publishing public directories must pass personal data in its possession relating to subscribers of other telephone service providers to a third-party undertaking whose activity consists in publishing a printed or electronic public directory or making such directories obtainable through directory enquiry services and which does not make the passing on of those data conditional on renewed consent from the subscribers. However, first, those subscribers must be informed, before the first inclusion of their data in a public directory, of the purpose of that directory and of the fact that those data may be communicated to another telephone service provider and, secondly, it must be guaranteed that those data will not, once passed on, be used for purposes other than those for which they were collected with a view to their first publication.  
35      For the purposes of reaching that conclusion, the Court held, in the light of recital 39 and of the wording of Article 12(2) and (3) of the Directive on privacy and electronic communications, that, where a subscriber has been informed by the undertaking which assigned him a telephone number of the possibility that his personal data may be passed to a third-party undertaking, with a view to being published in a public directory, and where he has consented to the publication of those data in such a directory, renewed consent is not needed from the subscriber for the passing of those same data to another undertaking which intends to publish a printed or electronic public directory, or to make such directories available for consultation through directory enquiry services, if it is guaranteed that the data in question will not be used for purposes other than those for which the data were collected with a view to their first publication. The consent given under Article 12(2) of that directive, by a subscriber who has been duly informed, to the publication of his personal data in a public directory relates to the purpose of that publication and thus extends to any subsequent processing of those data by third-party undertakings active in the market for publicly available directory enquiry services and directories, provided that such processing pursues that same purpose. The Court has stated in that regard that the wording of Article 12(2) of the Directive on privacy and electronic communications does not support the inference that the subscriber has a selective right to decide in favour of certain providers of publicly available directory enquiry services and directories (see, to that effect, judgment of 5 May 2011,   
Deutsche Telekom  
, C-543/09, EU:C:2011:279, paragraphs 62 to 65).  
36      The Court has added that, where a subscriber has consented to the passing of his personal data to a given undertaking with a view to their publication in a public directory of that undertaking, the passing of the same data to another undertaking intending to publish a public directory without renewed consent having been obtained from that subscriber is not capable of substantively impairing the right to protection of personal data, as recognised by Article 8 of the Charter of Fundamental Rights of the European Union (see, to that effect, judgment of 5 May 2011,   
Deutsche Telekom  
, C-543/09, EU:C:2011:279, paragraph 66).  
37      It follows from the foregoing that it is the purpose of the first publication of the subscriber’s personal data to which he gave his consent which is decisive for the purposes of determining the scope of that consent. It should be noted, in that regard, that Article 12(3) of the Directive on privacy and electronic communications provides that the Member States may require the consent of subscribers to be obtained also in respect of any purpose of a public directory other than the simple search of contact details of persons on the basis of their name and, where necessary, a limited number of other identifiers.  
38      Moreover, it should be noted that, regardless of where they are established in the European Union, undertakings which provide publicly available telephone directory enquiry services and directories operate within a highly harmonised regulatory framework making it possible to ensure throughout the European Union the same respect for requirements relating to the protection of subscribers’ personal data, resulting in particular from Article 25(5) of the Universal Service Directive and Article 1(1) and Article 12 of the Directive on privacy and electronic communications.  
39      In those circumstances, as the Advocate General stated in points 40 and 41 of his Opinion, there is no need to establish a difference in treatment according to whether the undertaking requesting the transfer of personal data relating to subscribers is established in the territory of those subscribers’ Member State or in another Member State, since that undertaking collects that data for purposes identical to those for which it was collected with a view to its first publication and, consequently, that transfer is covered by the consent that was given by those subscribers.  
40      Consequently, in the light of those considerations and those set out in paragraphs 23 to 30 of the present judgment, it is not necessary for the undertaking assigning telephone numbers to its subscribers to differentiate in the request for consent addressed to the subscriber according to the Member State to which the data concerning him could be sent.  
41      In the light of all the above considerations, the answer to the second question is that Article 25(2) of the Universal Service Directive must be interpreted as precluding an undertaking which makes telephone numbers available to subscribers, and which is obliged under national legislation to request those subscribers’ consent to the use of data relating to them for the purposes of supplying directory enquiry services and directories, from differentiating in the request for those subscribers’ consent to that use according to the Member State in which the undertakings requesting the information referred to in that provision provide those services.  
   
Costs  
42      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
1.        
Article 25(2) of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users’ rights relating to electronic communications networks and services (Universal Service Directive), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, must be interpreted as meaning that the concept of ‘requests’ in that article, covers also requests made by an undertaking, established in a Member State other than that in which the undertakings which assign telephone numbers to subscribers are established, which requests the relevant information possessed by those undertakings in order to provide publicly available telephone directory enquiry services and directories in that Member State and/or in other Member States.  
2.        
Article 25(2) of Directive 2002/22, as amended by Directive 2009/136, must be interpreted as precluding an undertaking which assigns telephone numbers to subscribers, and which is obliged under national legislation to request those subscribers’ consent to the use of data relating to them for the purposes of supplying directory enquiry services and directories, from differentiating in the request for those subscribers’ consent to that use according to the Member State in which the undertakings requesting the information referred to in that provision provide those services.

ID: 5babfa2f-eec1-4ce2-8272-8303ee65dafd

of 30 Nov -0001, C-667/21 (  
Krankenversicherung Nordrhein  
)  
  
  
  
  
Disclaimer

ID: 5df6e46d-eb44-4b26-9b5a-8db0cb8aa38b

of 28 Apr 2022, C-319/20 (  
Meta Platforms Ireland  
)  
   
JUDGMENT OF THE COURT (Third Chamber)  
28 April 2022 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 80 – Representation of the data subjects by a not-for-profit association – Representative action brought by a consumer protection association in the absence of a mandate and independently of the infringement of specific rights of a data subject – Action based on the prohibition of unfair commercial practices, the infringement of a consumer protection law or the prohibition of the use of invalid general terms and conditions)  
In Case C-319/20,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 28 May 2020, received at the Court on 15 July 2020, in the proceedings  
Meta Platforms Ireland Limited,   
formerly Facebook Ireland Limited,  
v  
Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.,  
THE COURT (Third Chamber),  
composed of A. Prechal, President of the Second Chamber, acting as President of the Third Chamber, J. Passer, F. Biltgen, L.S. Rossi (Rapporteur) and N. Wahl, Judges,  
Advocate General: J. Richard de la Tour,  
Registrar: M. Krausenböck, Administrator,  
having regard to the written procedure and further to the hearing on 23 September 2021,  
after considering the observations submitted on behalf of:  
–        Meta Platforms Ireland Limited, by H.-G. Kamann, M. Braun and H. Frey, Rechtsanwälte, and by V. Wettner, Rechtsanwältin,  
–        Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V., by P. Wassermann, Rechtsanwalt,  
–        for the German government, by D. Klebs and J. Möller, acting as Agents,  
–        the Austrian Government, by A. Posch and Dr G. Kunnert and J. Schmoll, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, P. Barros da Costa and L. Medeiros, acting as Agents,  
–        the European Commission, initially by F. Erlbacher, H. Kranenborg and D. Nardi, and subsequently by F. Erlbacher and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 2 December 2021,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 80(1) and (2) and Article 84(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (‘the GDPR’).  
2        The request has been made in proceedings between Meta Platforms Ireland Limited, formerly Facebook Ireland Limited, whose registered office is in Ireland, and Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (Federal Union of Consumer Organisations and Associations, Germany) (‘the Federal Union’) concerning the infringement by Meta Platforms Ireland of the German legislation on the protection of personal data constituting, at the same time, an unfair commercial practice, an infringement of a law relating to consumer protection and a breach of the prohibition of the use of invalid general terms and conditions.  
   
Legal context  
   
European Union law  
   
The GDPR  
3        Recitals 9, 10, 13 and 142 of the GDPR state:  
‘(9)      The objectives and principles of Directive [95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)] remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive [95/46].  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
…  
(13)      In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. …  
…  
(142)      Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject’s mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject’s behalf independently of the data subject’s mandate.’  
4        Article 1 of that regulation, entitled ‘Subject matter and objectives’, provides, in paragraph 1 thereof:  
‘This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.’  
5        Article 4(1) of the GDPR provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.’  
6        Chapter III of the GDPR, which includes Articles 12 to 23, is entitled ‘Rights of the data subject’.  
7        Article 12 of that regulation, headed ‘Transparent information, communication and modalities for the exercise of the rights of the data subject’, lay downs, in paragraph 1 thereof:  
‘The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.’  
8        Article 13 of the GDPR, entitled ‘Information to be provided where personal data are collected from the data subject’, provides, in paragraph 1(c) and (e) thereof:  
‘Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:  
…  
(c)      the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;  
…  
(e)      the recipients or categories of recipients of the personal data, if any …’  
9        Chapter VIII of that regulation, which comprises Articles 77 to 84, is entitled ‘Remedies, liability and penalties’.  
10      Article 77 of the GDPR, headed ‘Right to lodge a complaint with a supervisory authority’, provides, in paragraph 1 thereof:  
‘Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.’  
11      Article 78 of the GDPR, headed ‘Right to an effective judicial remedy against a supervisory authority’, lays down, in paragraph 1 thereof:  
‘Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.’  
12      Article 79 of the GDPR, headed ‘Right to an effective judicial remedy against a controller or processor’, provides, in paragraph 1 thereof:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’  
13      Article 80 of the GDPR, entitled ‘Representation of data subjects’, is worded as follows:  
‘1.      The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects’ rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.  
2.      Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject’s mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.’  
14      Article 82 of that regulation, headed ‘Right to compensation and liability’, provides, in paragraph 1 thereof:  
‘Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.’  
15      Article 84 of the GDPR, entitled ‘Penalties’, lays down, in paragraph 1 thereof:  
‘Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.’  
   
Directive 2005/29/EC  
16      The objective of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ 2005 L 149, p. 22) is, according to Article 1 thereof, to contribute to the proper functioning of the internal market and achieve a high level of consumer protection by approximating the laws, regulations and administrative provisions of the Member States on unfair commercial practices harming consumers’ economic interests.  
17      Under Article 5 of Directive 2005/29, entitled ‘Prohibition of unfair commercial practices’:  
‘1.      Unfair commercial practices shall be prohibited.  
2.      A commercial practice shall be unfair if:  
(a)      it is contrary to the requirements of professional diligence,  
and  
(b)      it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.  
…  
5.      Annex I contains the list of those commercial practices which shall in all circumstances be regarded as unfair. …’  
18      Article 11(1) of that directive, entitled ‘Enforcement’, provides:  
‘Member States shall ensure that adequate and effective means exist to combat unfair commercial practices in order to enforce compliance with the provisions of this Directive in the interest of consumers.  
Such means shall include legal provisions under which persons or organisations regarded under national law as having a legitimate interest in combating unfair commercial practices, including competitors, may:  
(a)      take legal action against such unfair commercial practices;  
and/or  
(b)      bring such unfair commercial practices before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings.  
It shall be for each Member State to decide which of these facilities shall be available and whether to enable the courts or administrative authorities to require prior recourse to other established means of dealing with complaints, including those referred to in Article 10. These facilities shall be available regardless of whether the consumers affected are in the territory of the Member State where the trader is located or in another Member State.  
…’  
19      Annex I to Directive 2005/29, which contains the list of unfair commercial practices in all circumstances, provides, in point 26 thereof:  
‘Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation. This is without prejudice to … [Directive 95/46] …’  
   
Directive 2009/22/EC  
20      Under Article 1 of Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers’ interests (OJ 2009 L 110, p. 30), entitled ‘Scope’:  
‘1.      The purpose of this Directive is to approximate the laws, regulations and administrative provisions of the Member States relating to actions for an injunction referred to in Article 2 aimed at the protection of the collective interests of consumers included in the Directives listed in Annex I, with a view to ensuring the smooth functioning of the internal market.  
2.      For the purposes of this Directive, an infringement means any act contrary to the Directives listed in Annex I as transposed into the internal legal order of the Member States which harms the collective interests referred to in paragraph 1.’  
21      Article 7 of Directive 2009/22, entitled ‘Provisions for wider action’, is worded as follows:  
‘This Directive shall not prevent Member States from adopting or maintaining in force provisions designed to grant qualified entities and any other person concerned more extensive rights to bring action at national level.’  
22      Annex I to Directive 2009/22 contains the list of EU directives referred to in Article 1 thereof. Point 11 of that annex refers to Directive 2005/29.  
   
Directive (EU) 2020/1828  
23      Recitals 11, 13 and 15 of Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ 2020 L 409, p. 1) state:  
‘(11)      This Directive should not replace existing national procedural mechanisms for the protection of collective or individual consumer interests. Taking into account their legal traditions, it should leave it to the discretion of the Member States whether to design the procedural mechanism for representative actions required by this Directive as part of an existing or as part of a new procedural mechanism for collective injunctive measures or redress measures, or as a distinct procedural mechanism, provided that at least one national procedural mechanism for representative actions complies with this Directive. … If there were procedural mechanisms in place at national level in addition to the procedural mechanism required by this Directive, the qualified entity should be able to choose which procedural mechanism to use.  
…  
(13)      The scope of this Directive should reflect recent developments in the field of consumer protection. Since consumers now operate in a wider and increasingly digitalised marketplace, achieving a high level of consumer protection requires that areas such as data protection, financial services, travel and tourism, energy, and telecommunications be covered by the Directive, in addition to general consumer law. …  
…  
(15)      This Directive should be without prejudice to the legal acts listed in Annex I and therefore it should not change or extend the definitions laid down in those legal acts or replace any enforcement mechanism that those legal acts might contain. For example, the enforcement mechanisms provided for in or based on [the GDPR] could, where applicable, still be used for the protection of the collective interests of consumers.’  
24      Article 2 of that directive, headed ‘Scope’, provides, in paragraph 1 thereof:  
‘This Directive applies to representative actions brought against infringements by traders of the provisions of Union law referred to in Annex I, including such provisions as transposed into national law, that harm or may harm the collective interests of consumers. This Directive is without prejudice to the provisions of Union law referred to in Annex I. …’  
25      Article 24(1) of that directive, entitled ‘Transposition’, provides:  
Member States shall adopt and publish, by 25 December 2022, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof.  
They shall apply those measures from 25 June 2023.  
…’  
26      Annex I to Directive 2020/1828, which contains the list of provisions of EU law referred to in Article 2(1) thereof, refers to the GDPR in point 56 thereof.  
   
German law  
   
Law on injunctions  
27      Under Paragraph 2 of the Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz – UKlaG) (Law on injunctions against infringements of consumer law and other infringements) of 26 November 2001 (BGBl. 2001 I, p. 3138), in the version applicable to the dispute in the main proceedings (‘the Law on Injunctions’):  
‘(1)      Any person who infringes rules in place to protect consumers (consumer protection laws), other than in the application or recommendation of general terms and conditions, may be subject to an order to cease and desist or a prohibition order in the interest of consumer protection. …  
(2)      For the purposes of this provision, “consumer protection laws” means, in particular:  
…  
11.      the rules defining lawfulness  
(a)      of the collection of personal data of a consumer by an undertaking or  
(b)      the processing or use of personal data which have been collected by a business in relation to a consumer,  
where the data are collected, processed or used for the purposes of publicity, market and opinion research, use by an information agency, a personality and usage profile establishment, of any other data business or for similar commercial purposes.’  
28      The Bundesgerichtshof (Federal Court of Justice, Germany) states that, under point 1 of the first sentence of Paragraph 3(1) of the Law on Injunctions, bodies with standing to bring proceedings, within the meaning of Paragraph 4 of that law, may, first, in accordance with Paragraph 1 of that law, seek an injunction against the use of invalid general terms and conditions under Paragraph 307 of the Bürgerliches Gesetzbuch (Civil Code) and, second, seek an injunction against infringements of consumer protection law, within the meaning of Paragraph 2(2) of that law.  
   
Law against unfair competition  
29      Paragraph 3(1) of the Gesetz gegen den unlauteren Wettbewerb (Law against unfair competition) of 3 July 2004 (BGB1. 2004 I, p. 1414), in the version applicable to the main proceedings (‘the Law against unfair competition’), provides:  
‘Unfair commercial practices shall be prohibited.’  
30      Paragraph 3a of the Law against unfair competition is worded as follows:  
‘A person shall be considered to be acting unfairly where he or she infringes a statutory provision that is also intended to regulate market behaviour in the interests of market participants and the infringement is liable to have a significantly adverse effect on the interests of consumers, other market participants or competitors.’  
31      Paragraph 8 of the Law against unfair competition lays down:  
‘(1)      Any commercial practice which is unlawful under Paragraph 3 or Paragraph 7 may give rise to an order to cease and desist and, in the event of recurrence, an order to refrain or a prohibition order. …  
…  
(3)      Applications for the injunctions referred to in subparagraph (1) may be made:  
…  
3.      by qualified entities which provide evidence that they are included in the list of qualified entities, in accordance with Paragraph 4 of the [Law on injunctions] …’  
   
The Law on Electronic Media  
32      The Bundesgerichtshof (Federal Court of Justice) states that Paragraph 13(1) of the Telemediengesetz (‘the Law on Electronic Media’) of 26 February 2007 (BGB1. 2007 I, p. 179) was applicable until the GDPR came into force. As from that date, that provision has been replaced by Articles 12 to 14 of the GDPR.  
33      Under the first sentence of Paragraph 13(1) of the Law on Electronic Media:  
‘From the outset of the use, the service provider shall inform the user in a universally comprehensible form of the mode, the extent and the purpose of the collection and use of personal data and of the processing of his or her data in States which do not come within the scope of [Directive 95/46] in so far as he or she has not already been so informed.’  
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
34      Meta Platforms Ireland, which manages the provision of services of the online social network Facebook in the European Union, is the controller of the personal data of users of that social network in the European Union. Facebook Germany GmbH, which has its registered office in Germany, promotes the sale of advertising space at the internet address www.facebook.de. The Facebook internet platform contains, inter alia, at the internet address www.facebook.de, an area called ‘App-Zentrum’ (‘App Center’) on which Meta Platforms Ireland makes available to users free games provided by third parties. When consulting the App Center of some of those games, an indication appears informing the user that the use of the application concerned enables the gaming company to obtain a certain amount of personal data and, by that use, permission is given for it to publish data on behalf of that user, such as his or her score and other information. The consequence of that use is that the user accepts the general terms and conditions of the application and its data protection policy. In addition, in the case of a specific game, it is stated that the application has permission to post the status, photos and other information on behalf of that user.  
35      The Federal Union, a body which has standing under Paragraph 4 of the Law on Injunctions, considers that the information provided by the games concerned in the App Center is unfair, in particular in terms of the failure to comply with the legal requirements which apply to the obtention of valid consent from the user under the provisions governing data protection. Moreover, it considers that the statement that   
   
the application has permission to publish certain personal information of the user on his or her behalf constitutes a general condition which unduly disadvantages the user.  
36      In that context, the Federal Union brought an action for an injunction before the Landgericht Berlin (Regional Court, Berlin, Germany) against Meta Platforms Ireland based on Paragraph 3a of the Law against unfair competition, the first sentence of point 11 of Paragraph 2(2) of the Law on Injunctions and the Civil Code. It brought that action independently of a specific infringement of a data subject’s right to protection of his or her data and without being mandated to do so by such a person.  
37      The Landgericht Berlin (Regional Court, Berlin) ruled against Meta Platforms Ireland, in accordance with the form of order sought by the Federal Union. The appeal brought by Meta Platforms Ireland before the Kammergericht Berlin (Higher Regional Court, Berlin, Germany) was dismissed. Meta Platforms Ireland then brought an appeal on a point of law (  
Revision  
) before the referring court against the dismissal decision adopted by the Kammergericht Berlin (Higher Regional Court, Berlin).  
38      The referring court considers that the action brought by the Federal Union is well founded, in so far as Meta Platforms Ireland infringed Paragraph 3a of the Law against unfair competition and the first sentence of point 11 of Paragraph 2(2) of the Law on Injunctions, and used an invalid general condition, within the meaning of Paragraph 1 of the Law on Injunctions.  
39      However, that court has doubts as to the admissibility of the action brought by the Federal Union. It takes the view that it cannot be ruled out that the Federal Union, which did indeed have standing to bring proceedings on the date on which it brought the action – on the basis of Paragraph 8(3) of the Law against unfair competition and point 1 of the first sentence of Paragraph 3(1) of the Law on Injunctions – lost that status during the proceedings, following the entry into force of the GDPR and, in particular, Article 80(1) and (2) and Article 84(1) thereof. If that were the case, the referring court would have to uphold the appeal on a point of law brought by Meta Platforms Ireland and dismiss the action of the Federal Union, since, under German procedural law, standing to bring proceedings must endure until the end of the proceedings at last instance.  
40      According to the referring court, the answer in that regard is not clear from the assessment of the wording, scheme and objectives of the provisions of the GDPR.  
41      As regards the wording of the provisions of the GDPR, the referring court notes that the existence of standing to bring proceedings of not-for-profit bodies, organisations or associations which have been properly constituted in accordance with the law of a Member State, pursuant to Article 80(1) of the GDPR, presupposes that the data subject has mandated a body, organisation or association for it to exercise on his or her behalf the rights referred to in Articles 77 to 79 of the GDPR and the right to compensation referred to in Article 82 of the GDPR where the law of a Member State so provides.  
42      The referring court states that standing to bring proceedings under Paragraph 8(3)(3) of the Law against unfair competition does not cover such an action brought on the basis of a mandate and on behalf of a data subject in order to assert his or her personal rights. On the contrary, it confers on an association, by virtue of a right peculiar to it and stemming from Paragraph 3(1) and Paragraph 3a of the Law against unfair competition, standing to bring proceedings on an objective basis against infringements of the provisions of the GDPR, independently of the infringement of specific rights of data subjects and of a mandate conferred by them.  
43      In addition, the referring court observes that Article 80(2) of the GDPR does not provide for an association’s standing to bring proceedings in order to secure the application, objectively, of the law on the protection of personal data since that provision presupposes that the rights of a data subject laid down in the GDPR have actually been infringed as a result of the processing of specific data.  
44      Furthermore, an association’s standing to bring proceedings, such as that provided for in Paragraph 8(3) of the Law against unfair competition, cannot result from Article 84(1) of the GDPR, under which the Member States are to lay down the rules on other penalties applicable to infringements of that regulation and are to take all measures necessary to ensure that they are implemented. The standing of an association, such as that referred to in Paragraph 8(3) of the Law against unfair competition, cannot be regarded as constituting a ‘penalty’ within the meaning of that provision of the GDPR.  
45      As regards the scheme of the provisions of the GDPR, the referring court considers that it may be inferred from the fact that it harmonised, inter alia, the powers of the supervisory authorities that it is principally for those authorities to verify the application of the provisions of that regulation. However, the expression ‘without prejudice to any other … remedy’, which appears in Article 77(1), Article 78(1) and (2) and Article 79(1) of the GDPR, may undermine the argument that oversight of the application of the law is exhaustively governed by that regulation.  
46      As regards the objective of the provisions of the GDPR, the referring court notes that the effectiveness of that regulation may support an argument in favour of associations having standing to bring proceedings on the basis of competition law, in accordance with Paragraph 8(3)(3) of the Law against unfair competition, independently of the infringement of specific rights of data subjects, since that would allow an additional opportunity to supervise the application of the law to remain, in order to ensure as high a level as possible of protection of personal data, in accordance with recital 10 of the GDPR. Nonetheless, accepting that associations have standing to bring proceedings under competition law may be considered to run counter to the objective of harmonisation pursued by the GDPR.  
47      In the light of those considerations, the Bundesgerichtshof (Federal Court of Justice) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
‘Do the rules in Chapter VIII, in particular in Article 80(1) and (2) and Article 84(1), of [the GDPR] preclude national rules which – alongside the powers of intervention of the supervisory authorities responsible for monitoring and enforcing the Regulation and the options for legal redress for data subjects – empower, on the one hand, competitors and, on the other, associations, entities and chambers entitled under national law, to bring proceedings for breaches of [the GDPR], independently of the infringement of specific rights of individual data subjects and without being mandated to do so by a data subject, against [the person responsible for that infringement] before the civil courts on the basis of the prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions?’  
   
Consideration of the question referred  
48      As a preliminary point, it should be noted that, as is apparent, in particular, from paragraph 36 and from paragraphs 41 to 44 above, the dispute in the main proceedings is between a consumer protection association, such as the Federal Union, and Meta Platforms Ireland and concerns the question whether such an association may bring proceedings against that company in the absence of a mandate granted to it for that purpose and independently of the infringement of specific rights of the data subjects.  
49      In those circumstances, as the Commission correctly observed in its written observations, the answer to the question referred for a preliminary ruling depends solely on the interpretation of Article 80(2) of the GDPR, since the provisions of Article 80(1) of the GDPR and of Article 84 of the GDPR are not relevant in the present case. First, the application of Article 80(1) of the GDPR presupposes that the data subject has mandated the not-for-profit body, organisation or association referred to in that provision to take on his or her behalf the legal measures provided for in Articles 77 to 79 of the GDPR. It is common ground that that is not the case in the main proceedings, since the Federal Union acts independently of any mandate from a data subject. Second, it is common ground that Article 84 of the GDPR concerns the administrative and criminal penalties applicable to infringements of that regulation, which is also not at issue in the main proceedings.  
50      Furthermore, it should be noted that the case in the main proceedings does not raise the question of a competitor’s standing to bring proceedings. Consequently, it is only necessary to answer the part of the question which relates to the standing to bring proceedings of associations, bodies and chambers authorised under national law, referred to in Article 80(2) of the GDPR.  
51      It follows that the question referred by the referring court must be understood as seeking to ascertain, in essence, whether Article 80(2) of the GDPR must be interpreted as precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of a data subject, against the person allegedly responsible for an infringement of the laws protecting personal data, by alleging infringement of the prohibition of unfair commercial practices, consumer protection legislation or the prohibition of the use of invalid general terms and conditions.  
52      In order to answer that question, it must be borne in mind that, as is apparent from recital 10 of the GDPR, that regulation seeks, inter alia, to ensure consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data throughout the European Union and to remove obstacles to flows of personal data within the European Union.  
53      In that context, Chapter VIII of that regulation governs, inter alia, the legal remedies enabling the protection of the data subject’s rights where his or her personal data have been the subject of processing that is allegedly contrary to the provisions of that regulation. The protection of those rights may thus be sought either directly by the data subject or by an authorised entity, whether there is a mandate to that end or not, pursuant to Article 80 of the GDPR.  
54      Thus, first of all, the data subject has the right to lodge a complaint himself or herself  
   
with a supervisory authority of a Member State or to bring an action before the national civil courts. More specifically, that data subject has the right to lodge a complaint with a supervisory authority, in accordance with Article 77 of the GDPR, the right to an effective judicial remedy against a supervisory authority, pursuant to Article 78 of the GDPR, the right to an effective judicial remedy against a controller or processor, provided for in Article 79 of the GDPR, and the right to obtain from the controller or processor compensation for the harm suffered, under Article 82 of the GDPR.  
55      Next, in accordance with Article 80(1) of the GDPR, the data subject has the right to mandate a not-for-profit body, organisation or association, subject to certain conditions, to lodge a complaint on his or her behalf or to exercise the rights referred to in the articles referred to above on his or her behalf.  
56      In accordance with Article 80(2) of the GDPR, Member States may provide that any body, organisation or association, independently of a data subject’s mandate granted by a data subject, has the right to lodge, in the Member State in question, a complaint with the supervisory authority, pursuant to Article 77 of that regulation, and to exercise the rights referred to in Articles 78 and 79 thereof, if it considers that the rights of a data subject under that regulation have been infringed as a result of the processing of personal data concerning him or her.  
57      In that regard, it should be noted that, as is apparent from Article 1(1) of the GDPR, read in the light, inter alia, of recitals 9, 10 and 13 thereof, that regulation seeks to ensure the harmonisation of national legislation on the protection of personal data which is, in principle, full. However, the provisions of that regulation make it possible for Member States to lay down additional, stricter or derogating national rules, which leave them a margin of discretion as to the manner in which those provisions may be implemented (‘opening clauses’).  
58      In that regard, it must be recalled that, according to the Court’s settled case-law, pursuant to Article 288 TFEU and by virtue of the very nature of regulations and of their function in the system of sources of EU law, the provisions of those regulations generally have immediate effect in the national legal systems without it being necessary for the national authorities to adopt measures of application. Nonetheless, some of those provisions may necessitate, for their implementation, the adoption of measures of application by the Member States (judgment of 15 June 2021,   
Facebook Ireland and Others  
, C-645/19, EU:C:2021:483, paragraph 110 and the case-law cited).  
59      That is the case, inter alia, of Article 80(2) of the GDPR, which leaves the Member States a discretion with regard to its implementation. Thus, in order for it to be possible to proceed with the representative action without a mandate provided for in that provision, Member States must make use of the option made available to them by that provision to provide in their national law for that mode of representation of data subjects.  
60      However, as the Advocate General observed, in points 51 and 52 of his Opinion, when the Member States exercise the option granted to them by such an opening clause, they must use their discretion under the conditions and within the limits laid down by the provisions of the GDPR and must therefore legislate in such a way as not to undermine the content and objectives of that regulation.  
61      In this instance, as was confirmed by the German Government at the hearing in the present case, the German legislature did not adopt, following the entry into force of the GDPR, particular provisions specifically designed to implement Article 80(2) of that regulation in its national law. The national legislation at issue in the main proceedings, adopted in order to transpose Directive 2009/22, already allows consumer protection associations to bring legal proceedings against the person allegedly responsible for an infringement of the laws protecting personal data. That government observes, moreover, that, in its judgment of 29 July 2019,   
Fashion ID   
(C-40/17, EU:C:2019:629), concerning the interpretation of the provisions of Directive 95/46, the Court held that those provisions do not preclude that national legislation.  
62      In those circumstances, as the Advocate General observed in point 60 of his Opinion, it is necessary, in essence, to ascertain whether the national rules at issue in the main proceedings fall within the scope of the discretion conferred on each Member State by Article 80(2) of the GDPR and thus to interpret that provision taking into account its wording and the scheme and objectives of that regulation.  
63      In that regard, it should be noted that Article 80(2) of the GDPR allows Member States to provide for a representative action mechanism against the person allegedly responsible for an infringement of the laws protecting personal data, while setting out a number of requirements at the level of the personal and material scope which must be complied with for that purpose.  
64      As regards, in the first place, the personal scope of such a mechanism, standing to bring proceedings is conferred on a body, organisation or association which meets the criteria set out in Article 80(1) of the GDPR. In particular, that provision refers to ‘not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects’ rights and freedoms with regard to the protection of their personal data’.  
65      It must be held that a consumer protection association, such as the Federal Union, may fall within the scope of that concept in that it pursues a public interest objective consisting in safeguarding the rights and freedoms of data subjects in their capacity as consumers, since the attainment of such an objective is likely to be related to the protection of the personal data of those persons.  
66      The infringement of the rules intended to protect consumers or to combat unfair commercial practices – infringement which a consumer protection association, such as the Federal Union, aims to prevent and penalise, inter alia by recourse to actions for an injunction provided for in the applicable national legislation – may be related, as in the present case, to the infringement of the rules on the protection of personal data of those consumers.  
67      As regards, in the second place, the material scope of that mechanism, the exercise of the representative action provided for in Article 80(2) of the GDPR by an entity meeting the conditions referred to in paragraph 1 of that article presupposes that that entity, independently of any mandate conferred on it, ‘considers that the rights of a data subject under [that r]egulation have been infringed as a result of the processing’ of his or her personal data.  
68      In that regard, it must be stated, first, that for the purposes of bringing a representative action, within the meaning of Article 80(2) of the GDPR, such an entity cannot be required to carry out a prior individual identification of the   
   
person specifically concerned by data processing that is allegedly contrary to the provisions of the GDPR.  
69      It is sufficient to note that the concept of ‘data subject’, within the meaning of Article 4(1) of that regulation, covers not only an ‘identified natural person’, but also an ‘identifiable natural person’, namely a natural person ‘who can be identified’, directly or indirectly, by reference to an identifier such as, inter alia, a name, an identification number, location data or an online identifier. In those circumstances, the designation of a category or group of persons affected by such treatment may also be sufficient for the purpose of bringing such representative action.  
70      Secondly, under Article 80(2) of the GDPR, the bringing of a representative action is also not subject to the existence of a specific infringement of the rights which a person derives from the data protection rules.  
71      As is apparent from the very wording of that provision, recalled in paragraph 67 of the present judgment, the lodging of a representative action presupposes only that the entity concerned ‘considers’ that the rights of a data subject laid down in that regulation have been infringed as a result of the processing of his or her personal data and therefore alleges the existence of data processing that is contrary to the provisions of that regulation.  
72      It follows that, in order to recognise that such an entity has standing to bring proceedings under that provision, it is sufficient to claim that the data processing concerned is liable to affect the rights which identified or identifiable natural persons derive from that regulation, without it being necessary to prove actual harm suffered by the data subject, in a given situation, by the infringement of his or her rights.  
73      Such an interpretation is consistent with the requirements stemming from Article 16 TFEU and Article 8 of the Charter of Fundamental Rights of the European Union and, thus, with the objective pursued by the GDPR consisting in ensuring effective protection of the fundamental rights and freedoms of natural persons and, in particular, of ensuring a high level of protection of the right of every person to the protection of personal data concerning him or her (see, to that effect, judgment of 15 June 2021,   
Facebook Ireland and Others  
, C-645/19, EU:C:2021:483, paragraphs 44, 45 and 91).  
74      Authorising consumer protection associations, such as the Federal Union, to bring, by means of a representative action mechanism, actions seeking to have processing contrary to the provisions of that regulation brought to an end, independently of the infringement of the rights of a person individually and specifically affected by that infringement, undoubtedly contributes to strengthening the rights of data subjects and ensuring that they enjoy a high level of protection.  
75      Furthermore, it should be noted that the bringing of such a representative action, in so far as it makes it possible to prevent a large number of infringements of the rights of data subjects by the processing of their personal data, could prove more effective than the action that a single person individually and specifically affected by an infringement of his or her right to the protection of his or her personal data may bring against the person responsible for that infringement.  
76      As the Advocate General observed in point 76 of his Opinion, the preventive function of actions brought by consumer protection associations, such as the Federal Union, could not be guaranteed if the representative action provided for in Article 80(2) of the GDPR allowed only the infringement of the rights of a person individually and specifically affected by that infringement to be invoked.  
77      In the third place, it is still necessary to ascertain, as requested by the referring court, whether Article 80(2) of the GDPR precludes the bringing of a representative action independently of a specific infringement of a right of a data subject and of a mandate conferred by that data subject, where infringement of data protection rules has been alleged in the context of an action seeking to review the application of other legal rules intended to ensure consumer protection.  
78      In that regard, it should be noted at the outset that, as has been observed, in essence, in paragraph 66 of the present judgment, the infringement of a rule relating to the protection of personal data may at the same time give rise to an infringement of rules on consumer protection or unfair commercial practices.  
79      Therefore, as the Advocate General observed in point 72 of his Opinion, that provision does not preclude the Member States from exercising the option it offers them in that consumer protection associations are entitled to take action against infringements of the rights provided for by the GDPR through, as the case may be, rules intended to protect consumers or combat unfair commercial practices, such as those provided for by Directive 2005/29 and Directive 2009/22.  
80      That interpretation of Article 80(2) of the GDPR is moreover supported by Directive 2020/1828 which repeals and replaces, as from 25 June 2023, Directive 2009/22. In that context, it must be observed that, in accordance with Article 2(1) thereof, Directive 2020/1828 applies to representative actions brought in relation to traders’ infringements of the provisions of EU law referred to in Annex I of that directive, which mentions the GDPR in point 56.  
81      It is true that Directive 2020/1828 is not applicable in the context of the dispute in the main proceedings and its transposition deadline has not yet expired. However, it contains several elements which confirm that Article 80 of the GDPR does not preclude the bringing of additional representative actions in the field of consumer protection.  
82      Although, as is apparent from recital 11 of that directive, it remains possible to provide a procedural mechanism for additional representative actions in the field of consumer protection, the application mechanisms provided for in the GDPR or based on that regulation, such as that provided for in Article 80 of that regulation, cannot be replaced or amended, as stated in recital 15 of that directive, and they may thus be used to protect the collective interests of consumers.  
83      In the light of all the foregoing considerations, the answer to the question referred is that Article 80(2) of the GDPR must be interpreted as not precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.  
   
Costs  
84      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Article 80(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as not precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.

ID: 5fe80383-39e5-4879-be9d-22b0721429a7

of 9 Feb 2023, C-560/21 (  
KISA  
)  
   
Judgment of the Court (Sixth Chamber) of 9 February 2023 (request for a preliminary ruling from the Bundesarbeitsgericht – Germany) – ZS v Zweckverband „Kommunale Informationsverarbeitung Sachsen“ KISA, Körperschaft des öffentlichen Rechts  
(Case C-560/21, KISA) 1  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 38(3) – Data protection officer – Prohibition on dismissing data protection officer for performing his or her tasks – Requirement for functional independence – National legislation prohibiting the dismissal of a data protection officer without just cause)  
Language of the case: German  
Referring court  
Bundesarbeitsgericht  
Parties to the main proceedings  
Applicant:  
 ZS  
Defendant:  
 Zweckverband „Kommunale Informationsverarbeitung Sachsen“ KISA, Körperschaft des öffentlichen Rechts  
Operative part of the judgment  
The second sentence of Article 38(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as not precluding national legislation which provides that a controller or a processor may dismiss a data protection officer who is a member of staff of that controller or processor solely where there is just cause, even if the dismissal is not related to the performance of that officer’s tasks, in so far as such legislation does not undermine the achievement of the objectives of that regulation.  
\_\_\_\_\_\_\_\_\_\_\_\_  
1 OJ C 37, 24.1.2022.  
   
  
  
  
  
Disclaimer

ID: 6112b5fc-6115-44d7-a9d1-2ff5b23eb7ed

of 22 Jun 2021, C-439/19 (  
Latvijas Republikas Saeima  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Processing of personal data relating to criminal convictions and offences   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness, fairness and transparency   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Processing of personal data relating to criminal convictions and offences   
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accuracy   
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Integrity and confidentiality   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness, fairness and transparency   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Processing of personal data relating to criminal convictions and offences   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accuracy   
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Integrity and confidentiality   
   
JUDGMENT OF THE COURT (Grand Chamber)  
22 June 2021 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Articles 5, 6 and 10 – National legislation providing for public access to personal data relating to penalty points imposed for road traffic offences – Lawfulness – Concept of ‘personal data relating to criminal convictions and offences’ – Disclosure for the purpose of improving road safety – Right of public access to official documents – Freedom of information – Reconciliation with the fundamental rights to respect for private life and to the protection of personal data – Re-use of data – Article 267 TFEU – Temporal effect of a preliminary ruling – Ability of a constitutional court of a Member State to maintain the legal effects of national legislation incompatible with EU law – Principles of primacy of EU law and of legal certainty)  
In Case C-439/19,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia), made by decision of 4 June 2019, received at the Court on 11 June 2019, in the proceedings brought by  
B  
other party:  
Latvijas Republikas Saeima,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, J.-C. Bonichot, A. Arabadjiev, E. Regan, M. Ilešič (Rapporteur) and N. Piçarra, Presidents of Chambers, E. Juhász, M. Safjan, D. Šváby, S. Rodin, F. Biltgen, K. Jürimäe, C. Lycourgos and P.G. Xuereb, Judges,  
Advocate General: M. Szpunar,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        the Latvian Government, initially by V. Soņeca and K. Pommere, and subsequently by K. Pommere, acting as Agents,  
–        the Netherlands Government, by M.K. Bulterman and M. Noort, acting as Agents,  
–        the Austrian Government, by J. Schmoll and G. Kunnert, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes, P. Barros da Costa, A.C. Guerra and I. Oliveira, acting as Agents,  
–        the Swedish Government, by C. Meyer-Seitz, H. Shev, H. Eklinder, R. Shahsavan Eriksson, A. Runeskjöld, M. Salborn Hodgson, O. Simonsson and J. Lundberg acting as Agents,  
–        the European Commission, by D. Nardi, H. Kranenborg and I. Rubene, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 17 December 2020,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Articles 5, 6 and 10 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’), of Article 1(2)(cc) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ 2003 L 345, p. 90), as amended by Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 (OJ 2013 L 175, p. 1) (‘Directive 2003/98’), and of the principles of primacy of EU law and legal certainty.  
2        The request has been made in proceedings brought by B concerning the legality of national legislation providing for public access to personal data relating to penalty points imposed for road traffic offences.  
   
Legal context  
   
EU law  
   
Directive 95/46/EC  
3        Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) was repealed by the GDPR, with effect from 25 May 2018. Article 3 of that directive, headed ‘Scope’, was worded as follows:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the [EU Treaty, in the version in force prior to the Treaty of Lisbon,] and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
…’  
   
The GDPR  
4        Recitals 1, 4, 10, 16, 19, 39, 50 and 154 of the GDPR state:  
‘(1)      The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.  
…  
(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.  
…  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
…  
(16)      This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.  
…  
(19)      The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council [of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89)]. …  
…  
(39)      … In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. … Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. …  
…  
(50)      The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. …  
…  
(154)      This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive [2003/98/EC] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.’  
5        Article 1 of the GDPR, headed ‘Subject matter and objectives’, provides:  
‘1.      This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.  
2.      This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.  
3.      The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.’  
6        Article 2 of the GDPR, headed ‘Material scope’, provides in paragraphs 1 and 2:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;  
(c)      by a natural person in the course of a purely personal or household activity;  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
7        As set out in Article 4 of the GDPR, headed ‘Definitions’:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person …;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;  
…’  
8        Article 5 of the GDPR, headed ‘Principles relating to processing of personal data’, states:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; … (“purpose limitation”);  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; … (“storage limitation”);  
(f)      processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
9        Article 6 of the GDPR, headed ‘Lawfulness of processing’, provides in paragraph 1:  
‘Processing shall be lawful only if and to the extent that at least one of the following applies:  
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
(d)      processing is necessary in order to protect the vital interests of the data subject or of another natural person;  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.’  
10      Article 10 of the GDPR, headed ‘Processing of personal data relating to criminal convictions and offences’, provides:  
‘Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.’  
11      Article 51 of the GDPR, headed ‘Supervisory authority’, states in paragraph 1:  
‘Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (“supervisory authority”).’  
12      Article 85 of the GDPR, headed ‘Processing and freedom of expression and information’, provides in paragraph 1:  
‘Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.’  
13      Article 86 of the GDPR, headed ‘Processing and public access to official documents’, provides:  
‘Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.’  
14      As set out in Article 87 of the GDPR, headed ‘Processing of the national identification number’:  
‘Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.’  
15      Article 94 of the GDPR provides:  
‘1.      Directive [95/46] is repealed with effect from 25 May 2018.  
2.      References to the repealed Directive shall be construed as references to this Regulation. …’  
   
Directive 2016/680  
16      Recitals 10, 11 and 13 of Directive 2016/680 state:  
‘(10)      In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.  
(11)      It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, [the GDPR] applies. [The GDPR] therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. …  
…  
(13) A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union …’  
17      Article 3 of Directive 2016/680 provides:  
‘For the purposes of this Directive:  
…  
7.      “competent authority” means:  
(a)      any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or  
(b)      any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;  
…’  
   
Directive 2003/98  
18      Recital 21 of Directive 2003/98 states:  
‘This Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive [95/46].’  
19      Article 1 of Directive 2003/98, headed ‘Subject matter and scope’, provides as follows:  
‘1.      This Directive establishes a minimum set of rules governing the re-use and the practical means of facilitating re-use of existing documents held by public sector bodies of the Member States.  
2.      This Directive shall not apply to:  
…  
(cc)      documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data;  
…  
3.      This Directive builds on and is without prejudice to access regimes in the Member States.  
4.      This Directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in Directive [95/46].  
…’  
   
L  
atvian law  
20      Article 96 of the Latvijas Republikas Satversme (Constitution of the Republic of Latvia; ‘the Latvian Constitution’) provides:  
‘Everyone has the right to respect for his or her private life, home and correspondence.’  
21      Under Article 1(5) of the Informācijas atklātības likums (Law on freedom of information) of 29 October 1998 (  
Latvijas Vēstnesis  
, 1998, No 334/335), re-use consists in the use of publicly accessible information, held and created by an authority, for commercial or non-commercial purposes other than the initial purpose for which the information was created, if that use is by a private party and does not involve tasks in the exercise of public authority.  
22      Under Article 4 of that law, publicly accessible information is information that does not fall within the category of information subject to restricted access.  
23      Article 5(1) of that law provides that information is subject to restricted access where it is intended for a restricted group of persons for the purpose of the performance of their tasks or professional duties and the disclosure or loss thereof, on account of its nature and content, hinders or may hinder an authority’s activities, or causes or may cause harm to statutorily protected interests of persons. Article 5(2) states that information is regarded as being subject to restricted access where, inter alia, it is so provided by law and Article 5(6) specifies that information that has already been published cannot be regarded as being information subject to restricted access.  
24      In accordance with Article 10(3) of the Law on freedom of information, publicly accessible information may be provided upon request. The applicant is not required to justify specifically his or her interest in obtaining the information, and may not be refused access on the ground that the information does not concern him or her.  
25      Article 141 of the Ceļu satiksmes likums (Law on road traffic) of 1 October 1997 (  
Latvijas Vēstnesis  
, 1997, No 274/276), in the version applicable at the material time (‘the Law on road traffic’), headed ‘Access to information kept in the national register of vehicles and their drivers …’, states in paragraph 2:  
‘Information relating … to a person’s right to drive vehicles, to fines for the commission of road traffic offences which have been imposed on a person but not paid within the time limits laid down by law and other information recorded in the national register of vehicles and their drivers … shall be regarded as information in the public domain.’  
26      Article 431 of the Law on road traffic, headed ‘Penalty points system’, provides in paragraph 1:  
‘In order to influence the behaviour of drivers of vehicles, by promoting safe driving and compliance with road traffic rules, and in order to reduce as far as possible the risks for human life, human health and a person’s property, administrative offences committed by drivers of vehicles shall be entered in the register of convictions and penalty points shall be entered in the national register of vehicles and their drivers.’  
27      In accordance with paragraphs 1 and 4 of Ministru kabineta noteikumi Nr. 551 ‘Pārkāpumu uzskaites punktu sistēmas piemērošanas noteikumi’ (Cabinet Regulation No 551 on the rules for application of the penalty points system) of 21 June 2004 (  
Latvijas Vēstnesis  
, 2004, No 102), penalty points for administrative offences committed in relation to road traffic by drivers of vehicles are automatically registered on the day upon which the period for appealing against the decision imposing an administrative penalty expires.  
28      Under paragraph 7 of that regulation, penalty points are removed when they have expired.  
29      By virtue of paragraph 12 of that regulation, depending on the number of penalty points, drivers are subject to measures such as warnings, road safety training or tests, or a driving ban for a specified period.  
30      As is apparent from Article 32(1) of the Satversmes tiesas likums (Law on the Constitutional Court) of 5 June 1996 (  
Latvijas Vēstnesis  
, 1996, No 103), a judgment of the Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia) is final and enforceable when it is delivered. In accordance with Article 32(3) of that law, a legal provision which the Latvijas Republikas Satversmes tiesa (Constitutional Court) has declared to be inconsistent with a higher-ranking rule of law is treated as void from the day of publication of the judgment of that court, unless the court decides otherwise.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
31      B is a natural person upon whom penalty points were imposed on account of one or more road traffic offences. In accordance with the Law on road traffic and Regulation No 551 of 21 June 2004, the Ceļu satiksmes drošības direkcija (Road Safety Directorate, Latvia) (‘the CSDD’) entered those penalty points in the national register of vehicles and their drivers.  
32      Since the information relating to those penalty points that was contained in the register was accessible to the public and moreover, according to B, had been disclosed, for purposes of re-use, to a number of economic operators, B lodged a constitutional complaint with the Latvijas Republikas Satversmes tiesa (Constitutional Court), in order for it to examine whether Article 141(2) of the Law on road traffic is consistent with the fundamental right to respect for private life laid down in Article 96 of the Latvian Constitution.  
33      The Latvijas Republikas Saeima (Parliament of the Republic of Latvia; ‘the Latvian Parliament’) was involved in the proceedings as the institution which had adopted the Law on road traffic. In addition, the CSDD, which processes the data relating to penalty points imposed for road traffic offences, was heard, as were the Datu valsts inspekcija (data protection authority), which is the supervisory authority, within the meaning of Article 51 of the GDPR, in Latvia, and a number of other authorities and persons.  
34      In the context of the main proceedings, the Latvian Parliament confirmed that, under Article 141(2) of the Law on road traffic, any person may obtain information relating to penalty points imposed on another person, either by enquiring directly at the CSDD or by using the services provided by commercial re-users.  
35      It stated that that provision is lawful because it is justified by the objective of improving road safety. That public interest requires that persons infringing traffic regulations, in particular those disregarding them systematically and in bad faith, be openly identified and that drivers of vehicles, by means of that transparency, be deterred from committing offences.  
36      Furthermore, that provision is justified by the right of access to information, laid down by the Latvian Constitution.  
37      The Latvian Parliament explained that, in practice, disclosure of the information contained in the national register of vehicles and their drivers is subject to the condition that the person requesting the information must provide the national identification number of the driver about whom he or she wishes to enquire. This precondition for obtaining information is attributable to the fact that, unlike the person’s name, which may be identical to the name of other persons, the national identification number is a unique identifier.  
38      The CSDD pointed out that Article 141(2) of the Law on road traffic does not impose any limits on either public access to or re-use of data relating to penalty points. As regards the contracts which it concludes with commercial re-users, the CSDD stated that they do not provide for legal transfer of the data and that re-users must ensure that the information transmitted to their customers does not exceed that which can be obtained from the CSDD. In addition, under those contracts the acquirer affirms that it will use the information obtained in accordance with the purposes indicated in the contract and in compliance with the legislation in force.  
39      The Datu valsts inspekcija (data protection authority) expressed its doubts as to whether Article 141(2) of the Law on road traffic is consistent with Article 96 of the Latvian Constitution which lays down the right to respect for private life. In its view, the importance and the objective of processing carried out on the basis of the provision at issue in the main proceedings are not clearly established, and it cannot therefore be ruled out that that processing is inappropriate or disproportionate. Whilst the statistics relating to road traffic accidents in Latvia show a decrease in the number of accidents, there is, however, no proof that the penalty points system and public access to information relating to it have contributed to that favourable development.  
40      The Latvijas Republikas Satversmes tiesa (Constitutional Court) notes, first of all, that the constitutional complaint concerns Article 141(2) of the Law on road traffic only in so far as that provision makes penalty points entered in the national register of vehicles and their drivers accessible to the public.  
41      It observes, next, that penalty points are personal data and that, when assessing the right to respect for private life laid down in Article 96 of the Latvian Constitution, account is to be taken of the GDPR and, more generally, of Article 16 TFEU and Article 8 of the Charter.  
42      As regards the objectives of the Latvian road traffic legislation, that court explains that it is in particular in order to promote road safety that offences committed by drivers, which are classified as administrative offences in Latvia, are entered in the register of convictions and that penalty points are entered in the national register of vehicles and their drivers.  
43      So far as concerns, in particular, the national register of vehicles and their drivers, it states that that register enables the number of road traffic offences committed to be ascertained and measures to be implemented in the light of their number. The system relating to penalty points entered in that register is thus intended to improve road safety, first, by enabling drivers of vehicles who disregard the road traffic rules systematically and in bad faith to be distinguished from drivers who commit offences occasionally. Second, such a system is also capable of influencing the conduct of road users in a preventive manner, by encouraging them to comply with the road traffic rules.  
44      That court observes that it is not in dispute that Article 141(2) of the Law on road traffic grants any person the right to request and obtain from the CSDD the information contained in the national register of vehicles and their drivers concerning the penalty points imposed on drivers. It confirms that, in practice, the information is provided to the person requesting it once that person indicates the national identification number of the driver concerned.  
45      The Latvijas Republikas Satversmes tiesa (Constitutional Court) then explains that, since penalty points are classified as publicly accessible information, they fall within the scope of the Law on freedom of information and that that information may therefore be re-used for commercial or non-commercial purposes other than the initial purpose for which the information was created.  
46      In order to interpret and apply Article 96 of the Latvian Constitution consistently with EU law, that court seeks to ascertain, first, whether information relating to penalty points is among the information referred to in Article 10 of the GDPR, that is to say, ‘personal data relating to criminal convictions and offences’. If it is, the view could be taken that Article 141(2) of the Law on road traffic fails to comply with the requirement contained in Article 10 of the GDPR that processing of the data to which that article relates can take place only ‘under the control of official authority’ or if there are ‘appropriate safeguards for the rights and freedoms of data subjects’.  
47      That court states that Article 8(5) of Directive 95/46, which left it to each Member State to determine whether the special rules on data relating to offences and criminal convictions should be extended to data relating to administrative offences and sanctions, was, from 1 September 2007, implemented in Latvia in such a way that personal data relating to administrative offences could, like data relating to criminal offences and convictions, be processed only by the persons, and in the circumstances, provided for by law.  
48      It adds that the scope of Article 10 of the GDPR must, in accordance with recital 4 of that regulation, be assessed in the light of the function of fundamental rights in society. In that respect, the objective of preventing a previous conviction from having an excessive adverse effect on a person’s private and professional life could apply both to criminal convictions and to administrative offences. Account should be taken, in this context, of the case-law of the European Court of Human Rights on the equiparation of certain administrative cases with criminal cases.  
49      The Latvijas Republikas Satversmes tiesa (Constitutional Court) raises, second, the question of the scope of Article 5 of the GDPR. It is unsure, in particular, whether the Latvian legislature has complied with the obligation, set out in Article 5(1)(f), requiring personal data to be processed with ‘integrity and confidentiality’. It points out that Article 141(2) of the Law on road traffic, which, by giving access to information relating to penalty points, makes it possible to ascertain whether a person has been found guilty of a road traffic offence, was not accompanied by specific measures ensuring the security of such data.  
50      That court seeks, third, to ascertain whether Directive 2003/98 is relevant when examining whether Article 141(2) of the Law on road traffic is compatible with the right to respect for private life. It is apparent from that directive that the re-use of personal data may be permitted only if that right is respected.  
51      Fourth, in the light of the Court of Justice’s case-law according to which the interpretation of EU law provided in preliminary rulings has   
erga omnes   
 and   
ex tunc  
 effects, the Latvijas Republikas Satversmes tiesa (Constitutional Court) is uncertain whether, if Article 141(2) of the Law on road traffic were to be incompatible with Article 96 of the Latvian Constitution, read in the light of the GDPR and the Charter, it could nevertheless maintain the temporal effects of Article 141(2) of that law until the date of delivery of its judgment, given the large number of legal relationships at issue.  
52      It states that, under Latvian law, a measure that it declares unconstitutional is to be considered void from the day of delivery of its judgment, unless it decides otherwise. It explains that it must, in that regard, strike a balance between the principle of legal certainty and the fundamental rights of the various parties concerned.  
53      In those circumstances, the Latvijas Republikas Satversmes tiesa (Constitutional Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must the expression “processing of personal data relating to criminal convictions and offences or related security measures”, used in Article 10 of [the GDPR], be interpreted as meaning that it includes the processing of information relating to penalty points recorded against drivers for motoring offences as provided for in the provision at issue?  
(2)      Irrespective of the answer to the first question, can the provisions of [the GDPR], in particular the principle of “integrity and confidentiality” referred to in Article 5(1)(f) thereof, be interpreted as meaning that they prohibit Member States from stipulating that information relating to penalty points recorded against drivers for motoring offences falls within the public domain and from allowing such data to be processed by being communicated?  
(3)      Must recitals 50 and 154, Article 5(1)(b) and Article 10 of [the GDPR] and Article 1(2)(cc) of Directive 2003/98 be interpreted as meaning that they preclude legislation of a Member State which allows information relating to penalty points recorded against drivers for motoring offences to be transmitted for the purposes of re-use?  
(4)      If any of the foregoing questions is answered in the affirmative, must the principle of the primacy of EU law and the principle of legal certainty be interpreted as meaning that it might be permissible to apply the provision at issue and maintain its legal effects until [the Satversmes tiesa (Constitutional Court) makes a final ruling]?’  
   
Consideration of the questions referred  
   
First  
 question  
54      By its first question, the referring court asks, in essence, whether Article 10 of the GDPR must be interpreted as applying to the processing of personal data relating to penalty points imposed on drivers of vehicles for road traffic offences, consisting in the public disclosure of such data.  
55      Under Article 10 of the GDPR, processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) is to be carried out only under the control of official authority or when the processing is authorised by EU or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.  
56      It should, therefore, first of all be determined whether the information relating to penalty points that is disclosed to third parties pursuant to the legislation at issue in the main proceedings constitutes ‘personal data’, within the meaning of Article 4(1) of the GDPR, and whether that disclosure constitutes ‘processing’ of such data, within the meaning of Article 4(2) of that regulation, that comes under its material scope as defined in Article 2.  
57      In the first place, it is apparent from the order for reference that Latvian legislation provides for the imposition of penalty points on drivers of vehicles who have committed a road traffic offence and upon whom a financial or other penalty has been imposed. Those points are entered by a public body, the CSDD, in the national register of vehicles and their drivers on the day upon which the period for appealing against the decision imposing that penalty expires.  
58      It is also apparent from the order for reference that road traffic offences and the penalties for punishing them fall within administrative law in Latvia and that the aim of imposing penalty points is not to inflict a further penalty but to heighten awareness of the drivers concerned, by encouraging them to adopt safer driving behaviour. When a certain number of penalty points is reached, the person concerned may be banned from driving for a specified period.  
59      It is, in addition, clear from the order for reference that the legislation at issue in the main proceedings obliges the CSDD to disclose information relating to the penalty points imposed on a given driver to any person who requests access to that information. The CSDD merely requires, for that purpose, that the person seeking the information duly identifies the driver concerned by providing his or her national identification number.  
60      It must therefore be found that the information relating to penalty points, which concerns an identified natural person, is ‘personal data’, within the meaning of Article 4(1) of the GDPR, and that its disclosure by the CSDD to third parties constitutes ‘processing’, within the meaning of Article 4(2) of the GDPR.  
61      In the second place, the disclosure of that information falls within the very broad definition, set out in Article 2(1), of the GDPR’s material scope and is not included in the processing of personal data that Article 2(2)(a) and (d) of the GDPR excludes from its material scope.  
62      First, Article 2(2)(a) of the GDPR provides that that regulation does not apply to the processing of personal data ‘in the course of an activity which falls outside the scope of Union law’. That exception to the applicability of the GDPR must, like the other exceptions laid down in Article 2(2), be interpreted strictly (see, to that effect, judgments of 9 July 2020,   
Land Hessen  
, C-272/19, EU:C:2020:535, paragraph 68, and of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 84).  
63      In that regard, Article 2(2)(a) of the GDPR is to be read in conjunction with Article 2(2)(b) thereof and recital 16, which states that that regulation does not apply to the processing of personal data in the context of ‘activities which fall outside the scope of Union law, such as activities concerning national security’ and ‘activities in relation to the common foreign and security policy of the Union’.  
64      It follows that Article 2(2)(a) and (b) of the GDPR represents partly a continuation of the first indent of Article 3(2) of Directive 95/46. Therefore, Article 2(2)(a) and (b) of the GDPR cannot be interpreted in broader terms than the exception resulting from the first indent of Article 3(2) of Directive 95/46, a provision which already excluded from that directive’s scope inter alia the processing of personal data taking place in the course ‘of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the [EU Treaty, in the version in force prior to the Treaty of Lisbon,] and in any case … processing operations concerning public security, defence, State security …’.  
65      As the Court has repeatedly held, only the processing of personal data in the course of an activity of the State or of State authorities which was expressly listed in Article 3(2) of Directive 95/46 or in the course of an activity which could be classified in the same category was excluded from the scope of that directive (see, to that effect, judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraphs 42 to 44; of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraphs 36 and 37; and of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 38).  
66      It follows that Article 2(2)(a) of the GDPR, read in the light of recital 16 thereof, must be regarded as being designed solely to exclude from the scope of that regulation the processing of personal data carried out by State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category, with the result that the mere fact that an activity is an activity characteristic of the State or of a public authority is not sufficient ground for that exception to be automatically applicable to such an activity (see, to that effect, judgment of 9 July 2020,   
Land Hessen  
, C-272/19, EU:C:2020:535, paragraph 70).  
67      The activities having the aim of safeguarding national security that are envisaged in Article 2(2)(a) of the GDPR encompass, in particular, as the Advocate General has also observed in essence in points 57 and 58 of his Opinion, those that are intended to protect essential State functions and the fundamental interests of society.  
68      However, activities relating to road safety do not pursue such an objective and consequently cannot be classified in the category of activities having the aim of safeguarding national security, which are envisaged in Article 2(2)(a) of the GDPR.  
69      Second, Article 2(2)(d) of the GDPR provides that that regulation does not apply to the processing of personal data ‘by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’. As is clear from recital 19 of the GDPR, the reason for that exception is that the processing of personal data for such purposes by the competent authorities is governed by a more specific EU legal act, namely Directive 2016/680, which was adopted on the same day as the GDPR. Directive 2016/680 defines ‘competent authority’ in Article 3(7) and such a definition must be applied, by analogy, to Article 2(2)(d) of the GDPR.  
70      It is apparent from recital 10 of Directive 2016/680 that the concept of ‘competent authority’ must be understood in relation to the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, in view of the arrangements which may prove necessary, in that regard, because of the specific nature of those fields. In addition, recital 11 of that directive explains that the GDPR applies to processing of personal data that is carried out by a ‘competent authority’, within the meaning of Article 3(7) of the directive, but for purposes other than those of the directive.  
71      In the light of the material available to the Court, it does not appear that, in carrying out the activities at issue in the main proceedings, which consist in disclosing to the public, for a road safety purpose, personal data relating to penalty points, the CSDD may be regarded as a ‘competent authority’, within the meaning of Article 3(7) of Directive 2016/680, and, therefore, that such activities may be covered by the exception laid down in Article 2(2) of the GDPR.  
72      Therefore, the disclosure by the CSDD of the personal data relating to penalty points imposed on drivers of vehicles for road traffic offences falls within the material scope of the GDPR.  
73      As to the applicability of Article 10 of the GDPR to such disclosure, the question is whether the information thereby disclosed constitutes personal data ‘relating to criminal convictions and offences or related security measures’, within the meaning of that provision, the processing of which ‘shall be carried out only under the control of official authority’, unless the processing is ‘authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects’.  
74      In that regard, it is to be noted that Article 10 of the GDPR is intended to ensure enhanced protection as regards processing which, because of the particular sensitivity of the data at issue, is liable to constitute a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 44).  
75      Since the data to which Article 10 of the GDPR refers relates to behaviour that gives rise to social disapproval, the grant of access to such data is liable to stigmatise the data subject and thereby to constitute a serious interference with his or her private or professional life.  
76      In the present instance, it is true that decisions of the Latvian authorities for the purpose of punishment of road traffic offences are, as the Latvian Government has stated in its replies to the Court’s questions, entered in the register of convictions, to which the public has access only in limited circumstances, and not in the register of vehicles and their drivers, to which Article 141(2) of the Law on road traffic gives free access. However, as the referring court pointed out, disclosure by the CSDD of personal data entered in the latter register that relate to penalty points enables the public to ascertain whether a given person has committed road traffic offences and, if so, to deduce the seriousness and frequency of those offences. Such a system for the disclosure of penalty points therefore effectively gives access to personal data relating to road traffic offences.  
77      In order to determine whether such access amounts to processing of personal data relating to ‘offences’, within the meaning of Article 10 of the GDPR, it must be pointed out, first, that that term refers exclusively to criminal offences, as is apparent inter alia from the history of the GDPR. Whilst the European Parliament had proposed the express inclusion in that provision of the words ‘administrative sanctions’ (OJ 2017 C 378, p. 430), that proposal was not adopted. That fact is all the more noteworthy because the provision that preceded Article 10 of the GDPR, namely Article 8(5) of Directive 95/46, which referred, in its first subparagraph, to ‘offences’ and ‘criminal convictions’, enabled the Member States, in its second subparagraph, to ‘provide that data relating to administrative sanctions … also be processed under the control of official authority’. It is thus clear from reading Article 8(5) as a whole that the term ‘offence’ referred only to criminal offences.  
78      Accordingly, it must be held that, in deliberately not including the adjective ‘administrative’ in Article 10 of the GDPR, the EU legislature intended to limit the enhanced protection provided for by that provision to the criminal field alone.  
79      As the Advocate General has observed in points 74 to 77 of his Opinion, that interpretation is borne out by the fact that a number of language versions of Article 10 of the GDPR make express reference to ‘criminal offences’, for example the versions in German (  
Straftaten  
), Spanish (  
infracciones penales  
), Italian (  
reati  
), Lithuanian (  
nusikalstamas veikas  
), Maltese (  
reati  
) and Dutch (  
strafbare feiten  
).  
80      Second, the fact that road traffic offences are classified as administrative in Latvia is not decisive when determining whether those offences are covered by Article 10 of the GDPR.  
81      In that regard, it should be pointed out that the terms of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union (judgments of 19 September 2000,   
Linster  
, C-287/98, EU:C:2000:468, paragraph 43, and of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraph 47).  
82      In the present instance, it is to be noted, first of all, that the GDPR does not contain any reference to national law so far as concerns the scope of the terms in Article 10 thereof, in particular the terms ‘offences’ and ‘criminal convictions’.  
83      Next, it is apparent from recital 10 of the GDPR that that regulation is intended to contribute to the accomplishment of an area of freedom, security and justice by ensuring a consistent and high level of protection of natural persons with regard to the processing of personal data, which requires the level of protection to be equivalent and homogeneous in all the Member States. It would be contrary to such an objective if the enhanced protection provided for in Article 10 of the GDPR applied to the processing of personal data relating to road traffic offences only in some Member States, and not in others, solely because those offences are not classified as criminal in the latter Member States.  
84      Finally, as the Advocate General has observed in point 84 of his Opinion, that finding is supported by recital 13 of Directive 2016/680 which states that ‘a criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union’.  
85      It follows that the concept of ‘criminal offence’, which is decisive for determining whether Article 10 of the GDPR is applicable to personal data relating to road traffic offences, such as the data at issue in the main proceedings, requires an autonomous and uniform interpretation throughout the European Union, having regard to the objective pursued by that provision and the context of which it forms part; the classification given by the Member State concerned to those offences is not conclusive in that regard as the classification may vary from one country to another (see, to that effect, judgment of 14 November 2013,   
Baláž  
, C-60/12, EU:C:2013:733, paragraphs 26 and 35).  
86      Third, it must be examined whether road traffic offences, such as those which give rise to entry in the register of vehicles and their drivers of the penalty points whose disclosure to third parties is provided for by the provision at issue, constitute a ‘criminal offence’, for the purposes of Article 10 of the GDPR.  
87      According to the Court’s case-law, three criteria are relevant for assessing whether an offence is criminal in nature. The first criterion is the legal classification of the offence under national law, the second is the intrinsic nature of the offence, and the third is the degree of severity of the penalty that the person concerned is liable to incur (see, to that effect, judgments of 5 June 2012,   
Bonda  
, C-489/10, EU:C:2012:319, paragraph 37; of 20 March 2018,   
Garlsson Real Estate and Others  
, C-537/16, EU:C:2018:193, paragraph 28; and of 2 February 2021,   
Consob  
, C-481/19, EU:C:2021:84, paragraph 42).  
88      Even in the case of offences which are not classified as ‘criminal’ by national law, the intrinsic nature of the offence in question and the degree of severity of the penalties to which it is liable to give rise may nevertheless result in its being criminal in nature (see, to that effect, judgment of 20 March 2018,   
Garlsson Real Estate and Others  
, C-537/16, EU:C:2018:193, paragraphs 28 and 32).  
89      As regards the criterion relating to the intrinsic nature of the offence, it must be ascertained whether the penalty at issue has a punitive purpose and the mere fact that it also pursues a deterrent purpose does not mean that it cannot be characterised as a criminal penalty. It is of the very nature of criminal penalties that they seek both to punish and to deter unlawful conduct. By contrast, a measure which merely repairs the damage caused by the offence at issue is not criminal in nature (see, to that effect, judgments of 5 June 2012,   
Bonda  
, C-489/10, EU:C:2012:319, paragraph 39, and of 20 March 2018,   
Garlsson Real Estate   
and Others  
, C-537/16, EU:C:2018:193, paragraph 33). It is not in dispute that the giving of penalty points for road traffic offences, and also the fines or other penalties to which the commission of those offences may give rise, are not intended only to repair any harm caused by those offences but also have a punitive purpose.  
90      So far as concerns the criterion relating to the degree of severity of the penalties to which the commission of those offences may give rise, it is to be noted, first of all, that only road traffic offences of a certain seriousness entail the giving of penalty points and that such offences are therefore liable to give rise to penalties of a certain severity. Next, the imposition of penalty points is generally additional to the penalty for the commission of such an offence, which, as has been noted in paragraph 58 above, is indeed true of the legislation at issue in the main proceedings. Finally, the accumulation of penalty points itself has legal consequences, such as the obligation to sit a test, or even a driving ban.  
91      This analysis is borne out by the case-law of the European Court of Human Rights according to which, notwithstanding the move towards ‘decriminalisation’ of road traffic offences in certain States, those offences must generally, in the light of the purpose, both deterrent and punitive, of the penalties imposed and the degree of severity that those penalties may have, be regarded as being criminal in nature (see, to that effect, ECtHR, 21 February 1984,   
Öztürk   
v.   
Germany  
, CE:ECHR:1984:0221JUD000854479, §§ 49 to 53; 29 June 2007,   
O’Halloran and Francis   
v.   
the   
United Kingdom  
, CE:ECHR:2007:0629JUD001580902, §§ 33 to 36; and 4 October 2016,   
Rivard   
v.   
Switzerland  
, CE:ECHR:2016:1004JUD002156312, §§ 23 and 24).  
92      The classification of road traffic offences which may result in the giving of penalty points as a ‘criminal offence’, for the purposes of Article 10 of the GDPR, is also consonant with the aim of that provision. The public disclosure of personal data relating to road traffic offences, including the penalty points imposed for committing them, is liable, in light of the fact that such offences compromise road safety, to give rise to social disapproval and to result in stigmatisation of the data subject, in particular where the penalty points reveal a certain seriousness or certain frequency of the offences.  
93      It follows that road traffic offences which may result in penalty points being given are covered by the term ‘offences’ in Article 10 of the GDPR.  
94      In the light of all the foregoing considerations, the answer to the first question referred is that Article 10 of the GDPR must be interpreted as applying to the processing of personal data relating to penalty points imposed on drivers of vehicles for road traffic offences.  
   
S  
econd  
 question  
95      By its second question, the referring court asks, in essence, whether the provisions of the GDPR must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to disclose those data to any person who requests them, without that person having to establish a specific interest in obtaining the data.  
96      All processing of personal data must comply, first, with the principles relating to processing of data set out in Article 5 of the GDPR and, second, with one of the principles relating to lawfulness of processing listed in Article 6 of that regulation (see, to that effect, judgment of 16 January 2019,   
Deutsche Post  
, C-496/17, EU:C:2019:26, paragraph 57 and the case-law cited).  
97      As regards the principles relating to processing of personal data, it is true that the referring court makes specific reference to the principles of ‘integrity’ and ‘confidentiality’ laid down in Article 5(1)(f) of the GDPR. Nevertheless, it is apparent from the doubts expressed by that court that it seeks to establish more generally whether the processing of personal data at issue in the main proceedings may be regarded as lawful in the light of all of the provisions of that regulation and, in particular, in the light of the principle of proportionality.  
98      It follows that account should also be taken, in the answer to be provided to the referring court, of the other principles set out in Article 5(1) of the GDPR, in particular of the principle of ‘data minimisation’ in Article 5(1)(c), according to which personal data are to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and which gives expression to the principle of proportionality (see, to that effect, judgment of 11 December 2019,   
Asociaţia de Proprietari bloc M5A-ScaraA  
, C-708/18, EU:C:2019:1064, paragraph 48).  
99      So far as concerns the principles relating to lawfulness of processing, Article 6 of the GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being considered lawful, processing must fall within one of the cases provided for in Article 6 (see, to that effect, judgment of 11 December 2019,   
Asociaţia de Proprietari bloc M5A-ScaraA  
, C-708/18, EU:C:2019:1064, paragraphs 37 and 38). The processing of personal data at issue in the main proceedings – namely the public disclosure of data relating to penalty points imposed for road traffic offences – carried out by the CSDD may fall within Article 6(1)(e) of the GDPR, under which processing is lawful if and to the extent that it is ‘necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’.  
100    Furthermore, since, as has been held in paragraph 94 above, personal data relating to penalty points imposed on drivers of vehicles for road traffic offences are covered by Article 10 of the GDPR, their processing is subject to the additional restrictions laid down in that provision. Thus, under that provision, processing of those data ‘shall be carried out only under the control of official authority’, unless it is ‘authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects’. Article 10 states, in addition, that ‘any comprehensive register of criminal convictions shall be kept only under the control of official authority’.  
101    In the present instance, it is not in dispute that the processing of personal data at issue in the main proceedings, namely the public disclosure of data relating to penalty points imposed for road traffic offences, is carried out by a public body, the CSDD, which is the controller within the meaning of Article 4(7) of the GDPR (see, by analogy, judgment of 9 March 2017,   
Manni  
, C-398/15, EU:C:2017:197, paragraph 35). However, it is also not in dispute that, once the data have been disclosed, they are consulted by the persons who requested their disclosure and, as the case may be, are stored or disseminated by those persons. Since that further data processing is no longer carried out ‘under the control’ of the CSDD or other official authority, the national law authorising disclosure of the data by the CSDD must provide for ‘appropriate safeguards for the rights and freedoms of data subjects’.  
102    Therefore, it is in the light both of the general rules governing lawfulness, in particular those laid down in Article 5(1)(c) and Article 6(1)(e) of the GDPR, and of the specific restrictions prescribed in Article 10 thereof that it should be examined whether national legislation such as that at issue in the main proceedings is consistent with that regulation.  
103    In that regard, it is to be noted that none of those provisions lays down a general and absolute prohibition preventing a public authority from being empowered, or indeed compelled, under national legislation to disclose personal data to persons requesting such data.  
104    Whilst Article 5(1)(c) of the GDPR requires the principle of ‘data minimisation’ to be observed when personal data are processed, it is clear from the wording of that provision that it is not intended to impose a general and absolute prohibition of that kind and that, in particular, it does not preclude personal data from being disclosed to the public where such disclosure is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, within the meaning of Article 6(1)(e) of that regulation. That is so even where the data in question are covered by Article 10 of the GDPR, provided that the legislation authorising the disclosure provides for appropriate safeguards for the rights and freedoms of data subjects (see, to that effect, judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 73).  
105    In that context, it should be borne in mind that the fundamental rights to respect for private life and to the protection of personal data are not absolute rights, but must be considered in relation to their function in society and be weighed against other fundamental rights. Limitations may therefore be imposed, so long as, in accordance with Article 52(1) of the Charter, they are provided for by law, respect the essence of the fundamental rights and observe the principle of proportionality. Under the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. They must apply only in so far as is strictly necessary and the legislation which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraphs 172 to 176).  
106    Therefore, in order to determine whether public disclosure of personal data relating to penalty points, such as the disclosure at issue in the main proceedings, is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, within the meaning of Article 6(1)(e) of the GDPR, and whether the legislation authorising such disclosure provides for appropriate safeguards for the rights and freedoms of data subjects, within the meaning of Article 10 of that regulation, it should be ascertained in particular whether, having regard to the seriousness of the interference with the fundamental rights to respect for private life and to the protection of personal data caused by that disclosure, the latter is justified, and in particular proportionate, for the purpose of achieving the objectives pursued.  
107    In the present instance, the Latvian Parliament, in its observations before the referring court, and the Latvian Government, in its observations before the Court of Justice, contend that the disclosure by the CSDD of personal data relating to penalty points to any person who so requests falls within the task in the public interest, entrusted to that body, of improving road safety and is intended, in that respect, in particular to enable identification of drivers of vehicles who systematically infringe the road traffic rules and to influence the conduct of road users by encouraging them to behave in accordance with those rules.  
108    The improvement of road safety is an objective of general interest recognised by the European Union (see, to that effect, judgment of 23 April 2015,   
Aykul  
, C-260/13, EU:C:2015:257, paragraph 69 and the case-law cited). Member States are therefore justified in classifying road safety as a ‘task carried out in the public interest’, within the meaning of Article 6(1)(e) of the GDPR.  
109    However, in order to satisfy the conditions imposed by that provision, it is necessary that the disclosure of personal data relating to penalty points entered in the register kept by the CSDD genuinely meets the objective of general interest of improving road safety, without going beyond what is necessary in order to achieve that objective.  
110    As recital 39 of the GDPR makes clear, that requirement of necessity is not met where the objective of general interest pursued can reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed in Articles 7 and 8 of the Charter, since derogations and limitations in relation to the principle of protection of such data must apply only in so far as is strictly necessary (see, to that effect, judgment of 11 December 2019,   
Asociaţia de Proprietari bloc M5A-ScaraA  
, C-708/18, EU:C:2019:1064, paragraphs 46 and 47).  
111    As is clear from the practice of the Member States, each of them has a large number of methods, including that of deterrent punishment of road traffic offences, in particular by depriving the drivers concerned of the right to drive a vehicle, a ban whose breach may in turn be punished by effective sentences, without the public disclosure of the adoption of such measures being necessary. It is also clear from the Member States’ practice that numerous preventive measures may, furthermore, be adopted, ranging from public awareness campaigns to the adoption of individual measures requiring a driver to undergo training and take tests, without the public disclosure of the adoption of such individual measures being necessary. However, it is not apparent from the documents before the Court that such measures had been examined and preferred by the Latvian legislature instead of the adoption of the rules at issue in the main proceedings.  
112    Furthermore, as has been pointed out in paragraph 92 above, the public disclosure of personal data relating to road traffic offences, including data relating to the penalty points imposed for committing them, is liable to constitute a serious interference with the fundamental rights to respect for private life and to the protection of personal data, since it may give rise to social disapproval and result in stigmatisation of the data subject.  
113    In the light, first, of the sensitivity of the data in question and the seriousness of that interference with the fundamental rights of data subjects to respect for private life and to the protection of personal data and, second, of the fact that, having regard to the findings in paragraph 111 above, it is not apparent that the objective of improving road safety cannot reasonably be achieved just as effectively by other less restrictive means, the necessity, in order to achieve that objective, of such a system of disclosure of personal data relating to penalty points imposed for road traffic offences cannot be regarded as established (see, by analogy, judgment of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 86).  
114    Thus, whilst it may be justified to distinguish drivers who disregard the road traffic rules systematically and in bad faith from drivers who commit offences occasionally, the view cannot, however, be taken that identification of the first category of drivers must, for the purpose of improving road safety, be carried out by or shared with the general public, with the result that it is even questionable whether the legislation at issue in the main proceedings is appropriate for achieving the first of the objectives referred to in paragraph 107 above.  
115    Moreover, it is apparent from the documents before the Court that the CSDD discloses to the public not only the data relating to penalty points imposed on drivers disregarding the road traffic rules systematically and in bad faith, but also the data relating to penalty points imposed on drivers committing offences occasionally. It is thus clear that, in providing for general public access to penalty points, the legislation at issue in the main proceedings in any event goes beyond what is necessary in order to achieve the objective of combatting the systematic disregard in bad faith of the road traffic rules.  
116    So far as concerns the second objective mentioned in paragraph 107 above pursued by the legislation at issue in the main proceedings, it is apparent from the documents before the Court that, whilst a downward trend in the number of road traffic accidents may have been observed in Latvia, there is no basis for concluding that that trend is connected with disclosure of the information relating to penalty points rather than to the establishment of the penalty points system in itself.  
117    The conclusion set out in paragraph 113 above is not invalidated by the fact that in practice the CSDD makes disclosure of the personal data at issue conditional on applicants stating the national identification number of the driver about whom they wish to enquire.  
118    Even if, as the Latvian Government has stated, the disclosure of national identification numbers by the public bodies keeping the population registers is subject to strict requirements and thus complies with Article 87 of the GDPR, the fact remains that the legislation at issue in the main proceedings, as applied by the CSDD, permits any person who knows the national identification number of a particular driver to obtain, without any further condition, the personal data relating to the penalty points that have been imposed on that driver. Such a disclosure regime is liable to lead to a situation in which those data are disclosed to persons who, for reasons unrelated to the objective of general interest of improving road safety, wish to find out about the penalty points that have been imposed on a given person.  
119    Nor is the conclusion set out in paragraph 113 above invalidated by the fact that the national register of vehicles and their drivers is an official document, within the meaning of Article 86 of the GDPR.  
120    Whilst, as follows from recital 154 of the GDPR, public access to official documents constitutes a public interest capable of justifying the disclosure of personal data contained in such documents, that access must nevertheless be reconciled with the fundamental rights to respect for private live and to the protection of personal data, as Article 86 indeed expressly requires. In the light in particular of the sensitivity of data relating to penalty points imposed for road traffic offences and of the seriousness of the interference with the fundamental rights of data subjects to respect for private life and to the protection of personal data, which is caused by the disclosure of such data, it must be held that those rights prevail over the public’s interest in having access to official documents, in particular the national register of vehicles and their drivers.  
121    Furthermore, for the same reason, the right to freedom of information referred to in Article 85 of the GDPR cannot be interpreted as justifying the disclosure to any person who so requests of personal data relating to penalty points imposed for road traffic offences.  
122    In the light of all the foregoing, the answer to the second question is that the provisions of the GDPR, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to make those data accessible to the public, without the person requesting access having to establish a specific interest in obtaining the data.  
   
Third  
 question  
123    By its third question, the referring court asks, in essence, whether the provisions of the GDPR, in particular Article 5(1)(b) and Article 10 thereof, and Article 1(2)(cc) of Directive 2003/98 must be interpreted as precluding national legislation which authorises the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to disclose those data to economic operators for re-use.  
124    As the referring court states, this question arises from the fact that the CSDD concludes contracts with economic operators pursuant to which it transmits to them the personal data relating to penalty points entered in the national register of vehicles and their drivers, in order, inter alia, to enable any person wishing to find out about the penalty points imposed on a particular driver to obtain such data not only from the CSDD but also from those economic operators.  
125    It is clear from the answer to the second question that the provisions of the GDPR, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to make those data accessible to the public, without the person requesting access having to establish a specific interest in obtaining the data.  
126    Those provisions must, for reasons identical to those set out in the answer to the second question, be interpreted as also precluding national legislation which authorises a public body to disclose data of that kind to economic operators in order for the data to be re-used and disclosed to the public by them.  
127    Finally, so far as concerns Article 1(2)(cc) of Directive 2003/98, to which the third question also refers, as the Advocate General has observed in points 128 and 129 of his Opinion that provision is not relevant for the purpose of determining whether the rules of EU law on the protection of personal data preclude legislation such as that at issue in the main proceedings.  
128    Irrespective of whether data relating to penalty points imposed on drivers for road traffic offences are covered by Directive 2003/98, the scope of the protection of those data must, in any event, be determined on the basis of the GDPR, as follows, first, from recital 154 of the GDPR and, second, from recital 21 and Article 1(4) of that directive, both read in conjunction with Article 94(2) of the GDPR. Article 1(4) of Directive 2003/98 provides, in essence, that that directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data inter alia under EU law, and in particular does not alter the obligations and rights set out in the GDPR.  
129    In the light of the foregoing, the answer to the third question is that the provisions of the GDPR, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which authorises the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to disclose those data to economic operators for re-use.  
   
Fourth   
question  
130    By its fourth question, the referring court asks, in essence, whether the principle of primacy of EU law must be interpreted as precluding the constitutional court of a Member State, before which a complaint has been brought challenging national legislation that proves, in the light of a preliminary ruling given by the Court of Justice, to be incompatible with EU law, from deciding, in accordance with the principle of legal certainty, that the legal effects of that legislation be maintained until the date of delivery of the judgment by which it rules finally on that constitutional complaint.  
131    As is apparent from the order for reference, this question has been referred on account of the large number of legal relationships affected by the national legislation at issue in the main proceedings and of the fact that, under Article 32(3) of the Law on the Constitutional Court and the case-law relating thereto, the referring court, in performing its task of ensuring a balance between the principle of legal certainty and the fundamental rights of the persons concerned, may limit the retroactive effect of its judgments in order to prevent them from seriously compromising the rights of others.  
132    In that regard, it should be recalled that the interpretation which, in the exercise of the jurisdiction conferred on it by Article 267 TFEU, the Court gives to rules of EU law clarifies and defines the meaning and scope of those rules as they must be or ought to have been understood and applied from the time of their entry into force. It is only exceptionally that the Court may, in application of the general principle of legal certainty inherent in the EU legal order, be moved to restrict for any person concerned the opportunity of relying on a provision which it has interpreted with a view to calling into question legal relationships established in good faith. Two essential criteria must be fulfilled before such a limitation can be imposed, namely that those concerned should have acted in good faith and that there should be a risk of serious difficulties (judgments of 6 March 2007,   
Meilicke  
, C-292/04, EU:C:2007:132, paragraphs 34 and 35; of 22 January 2015,   
Balazs  
, C-401/13 and C-432/13, EU:C:2015:26, paragraphs 49 and 50; and of 29 September 2015,   
Gmina Wrocław  
, C-276/14, EU:C:2015:635, paragraphs 44 and 45).  
133    As the Court has consistently held, such a restriction may be allowed only in the actual judgment ruling upon the interpretation sought. Indeed, there must necessarily be a single occasion when a decision is made on the temporal effects of the requested interpretation which the Court gives of a provision of EU law. The principle that a restriction may be allowed only in the actual judgment ruling upon that interpretation guarantees the equal treatment of the Member States and of other persons subject to EU law, under that law, and fulfils, at the same time, the requirements arising from the principle of legal certainty (judgment of 6 March 2007,   
Meilicke  
, C-292/04, EU:C:2007:132, paragraphs 36 and 37; see, to that effect, judgments of 23 October 2012,   
Nelson and Others  
, C-581/10 and C-629/10, EU:C:2012:657, paragraph 91, and of 7 November 2018,   
O’Brien  
, C-432/17, EU:C:2018:879, paragraph 34).  
134    Consequently, the temporal effects of a preliminary ruling given by the Court cannot depend on the date of delivery of the judgment by which the referring court rules finally on the main action, or even on the referring court’s assessment of the need to preserve the legal effects of the national legislation at issue.  
135    By virtue of the principle of primacy of EU law, rules of national law, even of a constitutional order, cannot be allowed to undermine the unity and effectiveness of EU law (see, to that effect, judgments of 26 February 2013,   
Melloni  
, C-399/11, EU:C:2013:107, paragraph 59, and of 29 July 2019,   
Pelham and Others  
, C-476/17, EU:C:2019:624, paragraph 78). Even assuming that overriding considerations of legal certainty are capable of leading, by way of exception, to a provisional suspension of the ousting effect which a directly applicable rule of EU law has on national law that is contrary thereto, the conditions of such a suspension can be determined solely by the Court (see, to that effect, judgment of 8 September 2010,   
Winner Wetten  
, C-409/06, EU:C:2010:503, paragraphs 61 and 67).  
136    In this instance, since a risk of serious difficulties resulting from the interpretation adopted by the Court in the present judgment has not been shown to exist and the criteria referred to in paragraph 132 above are cumulative, it is not appropriate to limit the judgment’s temporal effects.  
137    In the light of the foregoing, the answer to the fourth question is that the principle of primacy of EU law must be interpreted as precluding the constitutional court of a Member State, before which a complaint has been brought challenging national legislation that proves, in the light of a preliminary ruling given by the Court of Justice, to be incompatible with EU law, from deciding, in accordance with the principle of legal certainty, that the legal effects of that legislation be maintained until the date of delivery of the judgment by which it rules finally on that constitutional complaint.  
   
Costs  
138    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 10 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as applying to the processing of personal data relating to penalty points imposed on drivers of vehicles for road traffic offences.  
2.        
The provisions of Regulation (EU) 2016/679, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to make those data accessible to the public, without the person requesting access having to establish a specific interest in obtaining the data.  
3.        
The provisions of Regulation (EU) 2016/679, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which authorises the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to disclose those data to economic operators for re-use.  
4.        
The principle of primacy of EU law must be interpreted as precluding the constitutional court of a Member State, before which a complaint has been brought challenging national legislation that proves, in the light of a preliminary ruling given by the Court of Justice, to be incompatible with EU law, from deciding, in accordance with the principle of legal certainty, that the legal effects of that legislation be maintained until the date of delivery of the judgment by which it rules finally on that constitutional complaint.

ID: 6205aeee-6265-4618-85ce-746bef985714

of 1 Aug 2022, C-184/20 (  
Vyriausioji tarnybinės etikos komisija  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legal obligation   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Special categories of personal data   
   
JUDGMENT OF THE COURT (Grand Chamber)  
1 August 2022 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 52(1) – Directive 95/46/EC – Article 7(c) – Article 8(1) – Regulation (EU) 2016/679 – Point (c) of the first subparagraph of Article 6(1) and the second subparagraph of Article 6(3) – Article 9(1) – Processing necessary for compliance with a legal obligation to which the controller is subject – Objective of public interest – Proportionality – Processing of special categories of personal data – National legislation requiring publication on the internet of data contained in the declarations of private interests of natural persons working in the public service or of heads of associations or establishments receiving public funds – Prevention of conflicts of interest and of corruption in the public sector)  
In Case C-184/20,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania), made by decision of 31 March 2020, received at the Court on 28 April 2020, in the proceedings   
OT  
v  
Vyriausioji tarnybinės etikos komisija,  
third party:  
Fondas ‘Nevyriausybinių organizacijų informacijos ir paramos centras’,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, A. Prechal, K. Jürimäe, C. Lycourgos, N. Jääskinen, I. Ziemele and J. Passer, Presidents of Chambers, M. Ilešič (Rapporteur), J.-C. Bonichot, A. Kumin and N. Wahl, Judges,  
Advocate General: P. Pikamäe,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        the Lithuanian Government, by K. Dieninis and V. Vasiliauskienė, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and M. Russo, avvocato dello Stato,  
–        the Finnish Government, by M. Pere, acting as Agent,  
–        the European Commission, by S.L. Kalėda, H. Kranenborg and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 9 December 2021,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of point (e) of the first subparagraph of Article 6(1) and Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
2        The request has been made in proceedings between OT and the Vyriausioji tarnybinės etikos komisija (Chief Official Ethics Commission, Lithuania) (‘the Chief Ethics Commission’) concerning a decision of the latter finding that OT had failed to fulfil his obligation to lodge a declaration of private interests.  
   
Legal context  
   
I  
nternational  
 law  
   
United Nations Convention against Corruption   
3        The United Nations Convention against Corruption, which was adopted by resolution 58/4 of the United Nations General Assembly of 31 October 2003 and entered into force on 14 December 2005, has been ratified by all the Member States and was approved by the European Union by Council Decision 2008/801/EC of 25 September 2008 (OJ 2008 L 287, p. 1).  
4        Article 1 thereof states:  
‘The purposes of this Convention are:  
(a)      to promote and strengthen measures to prevent and combat corruption more efficiently and effectively;  
…  
(c)      to promote integrity, accountability and proper management of public affairs and public property.’  
5        Article 7(4) of the convention provides:  
‘Each State Party shall, in accordance with the fundamental principles of its domestic law, endeavour to adopt, maintain and strengthen systems that promote transparency and prevent conflicts of interest.’  
   
Criminal Law Convention on Corruption   
6        The Criminal Law Convention on Corruption, which was adopted by the Council of Europe on 27 January 1999 and has been ratified by all the Member States, states in its fourth recital:  
‘Emphasising that corruption threatens the rule of law, democracy and human rights, undermines good governance, fairness and social justice, distorts competition, hinders economic development and endangers the stability of democratic institutions and the moral foundations of society’.  
   
European   
Union  
 law  
   
Convention on the fight against corruption involving officials  
7        The Convention drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union (OJ 1997 C 195, p. 2), which entered into force on 28 September 2005, provides in Article 2, headed ‘Passive corruption’:  
‘1.      For the purposes of this Convention, the deliberate action of an official, who, directly or through an intermediary, requests or receives advantages of any kind whatsoever, for himself or for a third party, or accepts a promise of such an advantage, to act or refrain from acting in accordance with his duty or in the exercise of his functions in breach of his official duties shall constitute passive corruption.  
2.      Each Member State shall take the necessary measures to ensure that conduct of the type referred to in paragraph 1 is made a criminal offence.’  
8        Article 3 of that convention, headed ‘Active corruption’, is worded as follows:  
‘1.      For the purposes of this Convention, the deliberate action of whosoever promises or gives, directly or through an intermediary, an advantage of any kind whatsoever to an official for himself or for a third party for him to act or refrain from acting in accordance with his duty or in the exercise of his functions in breach of his official duties shall constitute active corruption.  
2.      Each Member State shall take the necessary measures to ensure that conduct of the type referred to in paragraph 1 is made a criminal offence.’  
   
Directive 95/46/EC  
9        Recitals 10, 30 and 33 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) stated:  
‘(10) … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; … for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;  
…  
(30)      … in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; …  
…  
(33)      … data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; … however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms’.  
10      The object of that directive was defined in Article 1, which stated:  
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
11      Article 2 of the directive provided:  
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…’  
12      Chapter II of Directive 95/46, headed ‘General rules on the lawfulness of the processing of personal data’, was divided into nine sections.  
13      In Section I, headed ‘Principles relating to data quality’, Article 6 of that directive was worded as follows:  
‘1.      Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. …  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
…  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
14      In Section II, headed ‘Criteria for making data processing legitimate’, Article 7 of the directive provided:  
‘Member States shall provide that personal data may be processed only if:  
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject; or  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or  
…’  
15      In Section III, headed ‘Special categories of processing’, Article 8 of the directive, relating to ‘the processing of special categories of data’, provided:  
‘1.      Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.  
…  
4.      Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.  
…’  
   
The GDPR  
16      As provided in Article 94(1) thereof, the GDPR repealed Directive 95/46 with effect from 25 May 2018. By virtue of Article 99(2), the GDPR applies from that date.  
17      Recitals 4, 10, 26, 35, 39 and 51 of the GDPR state:  
‘(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the [Charter of Fundamental Rights of the European Union (Charter)] as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.  
…  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. … Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. … This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data (“sensitive data”). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.  
…  
(26)      The principles of data protection should apply to any information concerning an identified or identifiable natural person. … To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. …  
…  
(35)      Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. …  
…  
(39)      … The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. …  
…  
(51)      Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. … Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.’  
18      Article 1 of the GDPR, headed ‘Subject matter and objectives’, provides in paragraph 2:  
‘This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.’  
19      Article 4 of the GDPR, headed ‘Definitions’, is worded as follows:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;   
…  
(15)      “data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;  
…’  
20      Chapter II of the GDPR, headed ‘Principles’, comprises Articles 5 to 11 of the regulation.  
21      Article 5, which concerns the ‘principles relating to processing of personal data’, provides in paragraph 1:  
‘Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; … (“purpose limitation”);  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
…’  
22      Article 6 of the GDPR, headed ‘Lawfulness of processing’, provides in paragraphs 1 and 3:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:   
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
…  
3.      The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.   
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. … The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.’  
23      Article 9 of the GDPR, headed ‘Processing of special categories of personal data’, provides in paragraphs 1 and 2:  
‘1.      Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.   
2.      Paragraph 1 shall not apply if one of the following applies:  
…  
(g)      processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;  
…’  
   
Lithuanian Law  
24      The Lietuvos Respublikos viešųjų ir privačių interesų derinimo valstybinėje tarnyboje įstatymas Nr. VIII-371 (Law No VIII-371 of the Republic of Lithuania on the reconciliation of public and private interests in the public service) of 2 July 1997 (Žin., 1997, No 67-1659), in the version in force at the material time (‘the Law on the reconciliation of interests’), has the aim, as stated in Article 1 thereof, of reconciling the private interests of persons working in the public service and the public interests of society, of ensuring that the public interest takes precedence when decisions are taken, of guaranteeing the impartiality of the decisions taken, and of preventing corruption from emerging and spreading in the public service.  
25      Pursuant to Article 2(1) of the Law on the reconciliation of interests, the term ‘persons working in the public service’ covers, amongst others, persons who work in public associations or establishments that receive finance from the budget or from funds of the State or of a local authority and who are vested with administrative powers.  
26      Article 3 of the Law on the reconciliation of interests, headed ‘Obligations of persons seeking to work, working or having worked in the public service’, provides in paragraphs 2 and 3:  
‘2.      Persons seeking to work or working in the public service and the other persons referred to in Article 4(1) of this Law shall declare their private interests.   
3.      Persons who have left the public service shall be subject to the restrictions laid down in Section 5 of this Law.’  
27      Article 4 of the Law on the reconciliation of interests, headed ‘Declaration of private interests’, provides in paragraph 1:   
‘Any person working in the public service and any person seeking to perform duties in the public service shall declare his or her private interests by lodging a declaration of private interests (‘declaration’) in accordance with the detailed rules laid down by this Law and other acts. …’  
28      As set out in Article 5 of the Law on the reconciliation of interests:  
‘1.      Persons declaring their private interests shall lodge their declaration electronically in accordance with the detailed rules established by the [Chief Ethics Commission] within 30 days from the date of their election, recruitment or appointment (except in the cases referred to in Article 4(2) of this Law and in paragraphs 2, 3 and 4 of this Article).  
2.      Persons seeking to work in the public service (with the exception of the persons referred to in Article 4(2) of this Law and persons whose data are classified as laid down by statute and/or who carry out intelligence, counter-espionage or criminal intelligence activity) shall lodge their declaration before the date of their election, recruitment or appointment, unless other legal acts otherwise provide.  
3.      Persons whose data are classified as laid down by statute and/or who carry out intelligence, counter-espionage or criminal intelligence activity shall lodge their declaration within 30 days from the date of their election, recruitment or appointment with the head of the institution (or legal person) within which they work or his or her authorised representative, in accordance with the detailed rules established by that institution (or legal person).  
4.      Members of public procurement panels, persons entrusted by the head of a contracting authority with the award of contracts under the simplified procedure and experts participating in public procurement procedures shall lodge their declaration of private interests electronically (if not already lodged) before their participation in public procurement procedures begins. A member of a public procurement panel, a person entrusted by the head of a contracting authority with the award of contracts under the simplified procedure or an expert participating in public procurement procedures who has not lodged a declaration of private interests shall not be entitled to participate in the procurement procedure and must be relieved of the duties concerned.  
5.      If the legal act laying down the operational arrangements of the institution (or legal person) in which the person works so provides, the declaration may be lodged not only with the head of that institution (or legal person) or his or her authorised representative, but also with the head – or his or her authorised representative – of a legal person subject or accountable to that institution (or legal person), or of another legal person.  
6.      The institutions authorised to have access to the declarations shall request and obtain them, in the cases and in accordance with the detailed rules laid down by legal acts, from the declarant’s place of work or the [Chief Ethics Commission].’  
29      Article 6 of the Law on the reconciliation of interests, headed ‘Content of the declaration’, states:  
‘1.      The declarant shall set out in his or her declaration the following data concerning the declarant and his or her spouse, cohabitee or partner:  
(1)      forename, surname, personal identification number, social security number, employer(s) and duties;  
(2)      legal person of which the declarant or his or her spouse, cohabitee or partner is a member;  
(3)      self-employed activity, as defined in the Law on personal income tax;  
(4)      membership of undertakings, establishments, associations or funds and the functions carried out, with the exception of membership of political parties and trade unions;  
(5)      gifts (other than those from close relatives) received during the last 12 calendar months if their value is greater than EUR 150;  
(6)      information about transactions concluded during the last 12 calendar months and other current transactions if the value of the transaction is greater than EUR 3 000;  
(7)      close relatives or other persons or data known by the declarant liable to give rise to a conflict of interests.  
2.      The declarant may omit data relating to his or her spouse, cohabitee or partner if they are living apart, do not form a common household and the declarant is therefore not in possession of those data.’  
30      Article 10 of the Law on the reconciliation of interests, headed ‘Public disclosure of data relating to private interests’, provides:  
‘1.      Data set out in the declarations of elected representatives and persons occupying political posts, State officials, judges, heads and deputy heads of State or local authority institutions, temporary officials of political (personal) trust, State officials performing the duties of the head and deputy head of subdivisions of institutions or establishments, heads and deputy heads of undertakings and budgetary authorities of the State or of a local authority, heads and deputy heads of public establishments or associations that receive finance from the budget or from funds of the State or of a local authority, employees of the Bank of Lithuania with powers of public administration (performing functions in relation to supervision of the financial markets, to the extrajudicial settlement of disputes between consumers and financial market participants, and other public administration functions), members of the supervisory or administrative board and managers and deputy managers of public or private companies limited by shares in which the State or a local authority owns shares conferring on it more than one half of the voting rights in the general meeting of shareholders, members of the administrative board of State or local authority undertakings, presidents and vice-presidents of political parties, unpaid consultants and assistants and advisers of elected representatives and of persons occupying political posts, experts approved by the committees of the Parliament of the Republic of Lithuania, members of ministerial advisory boards, members of the Compulsory Health Insurance Council, unpaid advisers of the Compulsory Health Insurance Council, members of the National Health Council, doctors, dentists and pharmacists working in budgetary authorities or public establishments of the State or of a local authority, in State or local authority undertakings or in undertakings in which the State or a local authority owns shares conferring on it more than one half of the voting rights in the general meeting of shareholders which hold a health-care or pharmacy licence, and members of public procurement panels, persons entrusted by the head of a contracting authority with the award of contracts under the simplified procedure and experts participating in public procurement procedures (with the exception of data set out in the declarations of persons whose data are classified as laid down by statute and/or who carry out intelligence, counter-espionage or criminal intelligence activity) shall be public and be published on the website of the [Chief Ethics Commission] in accordance with the detailed rules laid down by it. Where a person whose data are public loses the status of declarant, the [Chief Ethics Commission], on application by the person concerned, shall remove the declaration from its website.  
2.      The following data provided in the declaration cannot be made public: the personal identification number, the social security number, special personal data, and other data disclosure of which is prohibited by statute. In addition, the data of the other party to a transaction shall not be published where that party is a natural person.’  
31      As laid down in Article 22 of the Law on the reconciliation of interests, headed ‘Authorities and public servants responsible for monitoring’:  
‘The way in which persons to whom this Law is applicable apply it shall be monitored by:  
(1)      the [Chief Ethics Commission];  
(2)      the heads of the State or local authority institutions or establishments concerned or their authorised representatives;  
(3)      the head of the contracting authority or the persons authorised by him or her (as regards members of public procurement panels, persons entrusted by the head of a contracting authority with the award of contracts under the simplified procedure and experts participating in public procurement procedures);  
(4)      other State bodies, in accordance with the detailed rules laid down by legal acts.  
…  
3.      Where substantiated information has been obtained according to which a person is not complying with the requirements of this Law, the heads of the State or local authority institutions or establishments or their authorised representatives, or the collegial State or local authority institution, shall, on their own initiative or on the instruction of the [Chief Ethics Commission], investigate the official activity of the person working in the public service. The [Chief Ethics Commission] shall be informed of the outcome of the check and has the right to appraise whether the assessment of the relevant person’s conduct in the investigation report is consistent with the provisions of this Law. …’  
32      Article 2(5) of the Law of the Republic of Lithuania on the reconciliation of public and private interests, in the version in force from 1 January 2020 (‘the Law on the reconciliation of interests as amended’), a provision which defines the term ‘persons working in the public service’, no longer refers, amongst such persons, to persons who work in public associations or establishments that receive finance from the budget or from funds of the State or of a local authority and who are vested with administrative powers.   
33      Article 4(3) of the Law on the reconciliation of interests as amended states:  
‘The provisions of this Law concerning the declaration of private interests and Articles 11 and 13 of this Law shall also be applicable:  
…  
(8)      to the head of a contracting authority or a contracting entity (together, “a contracting entity”), members of public procurement panels of a contracting entity, persons entrusted by the head of a contracting entity with the award of contracts under the simplified procedure, experts participating in public procurement procedures, and persons initiating a concession … at a contracting entity in the procurement, waste water treatment, energy, transport or postal services sector;  
…’  
34      As set out in Article 2(8) of the Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas Nr. I-1374 (Law No I-1374 of the Republic of Lithuania on the legal protection of personal data) of 11 June 1996 (Žin., 1996, No 63-1479), in the version in force until 16 July 2018:   
‘“Special personal data” shall mean data relating to a natural person’s racial or ethnic origin, political, religious, philosophical or other convictions, trade union membership, health or sex life, and information concerning a criminal conviction of that person.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
35      The Chief Ethics Commission is a public authority responsible inter alia for ensuring the application of the Law on the reconciliation of interests and, in particular, for collecting and checking declarations of private interests.  
36      OT serves as the director of QP, an establishment governed by Lithuanian law in receipt of public funds which operates in the field of environmental protection.  
37      By a decision of 7 February 2018, the Chief Ethics Commission found that, by failing to lodge a declaration of private interests, OT had infringed Article 3(2) and Article 4(1) of the Law on the reconciliation of interests.   
38      On 6 March 2018, OT brought an action for annulment of that decision before the referring court.   
39      In support of the action, OT submits, first, that he is not among the persons, as referred to in Article 2(1) of the Law on the reconciliation of interests, who are subject to the obligation to declare private interests. He states that, in his capacity as director of QP, he is vested with no powers of public administration and does not provide any public service to the population. Furthermore, QP, as a non-governmental organisation, carries out its activity independently of the public authorities.  
40      Second, and in any event, even if he is required to lodge a declaration of private interests, OT contends that its publication would adversely affect both his right to respect for private life and that of the other persons whom he would, as the case may be, be required to mention in his declaration.  
41      The Chief Ethics Commission asserts that, in so far as OT was vested with administrative powers in an establishment in receipt of financing from EU structural funds and the budget of the Lithuanian State, he was required to lodge a declaration of private interests, despite his not being an official and even if he did not exercise any powers of public administration. In addition, the Chief Ethics Commission observes that, whilst publication of such a declaration is liable to constitute an interference in the private life of OT and his spouse, that interference is provided for by the Law on the reconciliation of interests.  
42      The referring court has doubts as to whether the regime laid down by the Law on the reconciliation of interests is compatible with points (c) and (e) of the first subparagraph of Article 6(1) and Article 6(3) of the GDPR and with Article 9(1) thereof. It takes the view that the personal data contained in a declaration of private interests are liable to reveal information on the private life of the declarant and his or her spouse and of the declarant’s children, with the result that their disclosure is capable of infringing the right of the data subjects to respect for their private life. Indeed, those data are liable to reveal particularly sensitive information, such as the fact that the data subject is cohabiting or is living with another person of the same sex, the disclosure of which might well result in significant nuisance in the private life of those persons. The data concerning presents received and transactions carried out, by the declarant and his or her spouse, cohabitee or partner, also reveal certain details of their private life. Moreover, the data concerning close relatives or acquaintances of the declarant who may give rise to a conflict of interests reveal information about the declarant’s family and personal relationships.  
43      According to the referring court, whilst the Law on the reconciliation of interests has the objective of ensuring that the principle of transparency is observed when public functions are performed, in particular when decisions concerning implementation of the public interest are adopted, publication on the internet of matters capable of affecting the adoption of such decisions is not necessary in order to achieve that objective. Communication of the personal data to the bodies envisaged in Article 5 of that law and the monitoring task that is assigned to the organs referred to in Article 22 thereof constitute measures sufficient to ensure that that objective is achieved.  
44      In those circumstances, the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must the condition laid down in [point (e) of the first subparagraph of Article 6(1)] of the [GDPR] that processing [of the personal data] is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, with regard to the requirements laid down in Article 6(3) of [that regulation], including the requirement that the Member State law must meet an objective of public interest and be proportionate to the legitimate aim pursued, and also with regard to Articles 7 and 8 of the Charter, be interpreted as meaning that national law may not require the disclosure of declarations of private interests and their publication on the website of the controller (the [Chief Ethics Commission]), thereby providing access to those data to all individuals who have access to the internet?  
(2)      Must the prohibition of the processing of special categories of personal data established in Article 9(1) of the [GDPR], regard being had to the conditions established in Article 9(2) of [that regulation], including the condition established in point (g) thereof that processing [of the personal data] must be necessary for reasons of substantial public interest, on the basis of EU or Member State law which must be proportionate to the aim pursued, must respect the essence of the right to data protection and must provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, be interpreted, also with regard to Articles 7 and 8 of the Charter, as meaning that national law may not require the disclosure of data relating to declarations of private interests which may disclose personal data, including data which make it possible to determine a person’s political views, trade union membership, sexual orientation and other personal information, and their publication on the website of the controller (the [Chief Ethics Commission]), providing access to those data to all individuals who have access to the internet?’  
   
The admissibility of the request for a preliminary ruling  
45      The Lithuanian Government and the European Commission have stated that, following the amendment of the Law on the reconciliation of interests, which entered into force on 1 January 2020, the applicant in the main proceedings is no longer a person to whom that law applies.  
46      In addition, the Commission observes that, in a judgment of 20 September 2018, the Lietuvos Respublikos Konstitucinis Teismas (Constitutional Court of the Republic of Lithuania), which the referring court had requested to assess the constitutionality of certain provisions of the Law on the reconciliation of interests, found that Article 10 thereof, which requires the data relating to private interests to be published, was not at issue in the main proceedings.  
47      In that regard, it should be recalled that, in accordance with settled case-law, the procedure provided for in Article 267 TFEU is an instrument of cooperation between the Court of Justice and the national courts, by means of which the Court provides the national courts with the points of interpretation of EU law which they need in order to decide the disputes before them (judgment of 12 March 1998,   
Djabali  
, C-314/96, EU:C:1998:104, paragraph 17, and order of 3 December 2020,   
Fedasil  
, C-67/20 to C-69/20, not published, EU:C:2020:1024, paragraph 18).  
48      In accordance with equally settled case-law, questions on the interpretation of EU law referred by a national court in the factual and legislative context which that court is responsible for defining, and the accuracy of which is not a matter for the Court to determine, enjoy a presumption of relevance. The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 22 February 2022,   
Stichting Rookpreventie Jeugd and Others  
, C-160/20, EU:C:2022:101, paragraph 82 and the case-law cited).  
49      In the present instance, it must be pointed out that, in response to a request by the Court for information, the referring court explained, first, that the legality of the decision at issue in the main proceedings has to be assessed in the light of the national provisions in force on the date of that decision’s adoption. The Law on the reconciliation of interests included amongst the persons who had to lodge a declaration of private interests those who work in public associations or establishments that receive finance from the budget or from funds of the State or of a local authority and who are vested with administrative powers.  
50      The referring court stated, furthermore, that although the applicant in the main proceedings can no longer be equated to a person working in the public service, within the meaning of the Law on the reconciliation of interests as amended, he is nevertheless capable of falling within the category of persons that is referred to in Article 4(3)(8) of that law and that, on that basis, he may be required to lodge a declaration of private interests.  
51      Second, the referring court stated that the main proceedings are not affected by the judgment of the Lietuvos Respublikos Konstitucinis Teismas (Constitutional Court of the Republic of Lithuania) of 20 September 2018, by which it declared that the referring court’s request that it rule on whether Article 10(1) and (2) of the Law on the reconciliation of interests is consistent with the Constitution of the Republic of Lithuania and the constitutional principle of proportionality was inadmissible on the ground that the question to be decided in the main proceedings relates not to the public disclosure of the data provided in declarations of private interests, but to the obligation to lodge such a declaration.  
52      The referring court explained that, even though the question to be decided in the main proceedings is indeed, as the Lietuvos Respublikos Konstitucinis Teismas (Constitutional Court of the Republic of Lithuania) stated, whether the applicant in the main proceedings infringed Article 3(2) and Article 4(1) of the Law on the reconciliation of interests because he failed to comply with the obligation to lodge a declaration of private interests, in order to review the legality of the decision at issue in the main proceedings it is necessary to take account of the mandatory consequences, resulting from the application of Article 10 of that law, of the lodging of such a declaration, namely the publication on the Chief Ethics Commission’s website of certain data contained in the declaration, since the applicant in the main proceedings pleads in support of his action for annulment of that decision that that publication is unlawful.  
53      In the light of the information thereby provided by the referring court, the matters put forward by the Lithuanian Government and the Commission are not sufficient to rebut the presumption of relevance enjoyed by the questions referred and it cannot be considered to be quite obvious that the interpretation of provisions of EU law that is sought bears no relation to the actual facts of the main action or its purpose, or that the problem is hypothetical, as the referring court may take account of that interpretation for the purpose of adopting its decision. Furthermore, the Court has before it the factual and legal material necessary to give a useful answer to the questions submitted to it.  
54      Therefore the request for a preliminary ruling is admissible.  
   
Consideration of the questions referred  
   
The   
applicable  
 law   
   
ratione temporis  
55      By its questions, the referring court requests interpretation of the GDPR. In accordance with Article 99(2) thereof, the GDPR became applicable on 25 May 2018, the date with effect from which, by virtue of Article 94(1), it repealed Directive 95/46.  
56      Consequently, the decision at issue in the main proceedings, which was adopted by the Chief Ethics Commission on 7 February 2018, was governed by Directive 95/46.  
57      However, it is apparent from the documents before the Court that, by that decision, the Chief Ethics Commission alleged that the applicant in the main proceedings had failed to lodge a declaration of private interests, in breach of the Law on the reconciliation of interests. That being so, in the light of the information referred to in paragraph 50 of the present judgment and in the absence of anything to indicate that the applicant in the main proceedings lodged such a declaration before 25 May 2018, that is to say, the date on which the GDPR became applicable, the possibility remains that that regulation is applicable   
ratione temporis   
 to the dispute in the main proceedings, a matter which is for the referring court to determine.  
58      Furthermore, there is no need to distinguish between the provisions of Directive 95/46 and those of the GDPR referred to in the two questions referred for a preliminary ruling, as reformulated, since the purport of those provisions must be regarded as similar for the purposes of the interpretation that the Court is required to give in the present case (see, by analogy, judgment of 21 November 2013,   
Dixons Retail  
, C-494/12, EU:C:2013:758, paragraph 18).  
59      Therefore, in order to provide useful answers to the questions submitted by the referring court, they should be examined on the basis of both Directive 95/46 and the GDPR.  
   
The first   
question  
60      By its first question, the referring court asks, in essence, whether Article 7(c) and (e) of Directive 95/46 and points (c) and (e) of the first subparagraph of Article 6(1) and Article 6(3) of the GDPR, read in the light of Articles 7 and 8 of the Charter, must be interpreted as precluding a national provision that provides for the placing online of personal data contained in the declaration of private interests that any head of an establishment receiving public funds is required to lodge with the national authority responsible for collecting such declarations and checking their content.  
61      It should be noted at the outset that, under Article 1(1) of Directive 95/46, read in conjunction with recital 10 thereof, and Article 1(2) of the GDPR, read in conjunction with recitals 4 and 10 thereof, that directive and that regulation have the objective in particular of ensuring a high level of protection of the fundamental rights and freedoms of natural persons with respect to the processing of personal data; that right is also recognised in Article 8 of the Charter and is closely connected to the right to respect for private life, enshrined in Article 7 of the Charter.  
62      To that end, Chapter II of Directive 95/46 and Chapters II and III of the GDPR set out the principles governing the processing of personal data and the rights of the data subject which the processing must observe. In particular, all processing of personal data was required, before the GDPR was applicable, to comply with the principles relating to data quality and the criteria for making data processing legitimate set out in Articles 6 and 7 of that directive and, once the GDPR was applicable, to comply with the principles relating to processing of data and the conditions governing lawfulness of processing listed in Articles 5 and 6 of that regulation (see, to that effect, judgments of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 96, and of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 50).  
63      In the present instance, Article 10(1) of the Law on the reconciliation of interests provides that the Chief Ethics Commission is to publish on its website the information set out in the declarations of private interests which are submitted by the public officials referred to in that provision and the content of which is defined in Article 6(1) of that law, with the exception of the information listed in Article 10(2) thereof.  
64      It should be pointed out, in that regard, that the questions referred to the Court relate solely to the publication, on the Chief Ethics Commission’s website, of the information set out in the declaration of private interests that the head of an establishment receiving public funds is required to lodge, and not to the obligation to declare in itself or to the publication of a declaration of interests in other circumstances.   
65      Where information intended to be published on the Chief Ethics Commission’s website relates to natural persons identified by their forename and surname, it constitutes personal data, within the meaning of Article 2(a) of Directive 95/46 and Article 4(1) of the GDPR, and the fact that that information was provided in the context of the declarant’s professional activity does not mean that it cannot be so characterised (judgment of 9 March 2017,   
Manni  
, C-398/15, EU:C:2017:197, paragraph 34 and the case-law cited). Furthermore, the operation of loading personal data on an internet page constitutes processing, within the meaning of Article 2(b) of Directive 95/46 and Article 4(2) of the GDPR (see, to that effect, judgment of 1 October 2015,   
Weltimmo  
, C-230/14, EU:C:2015:639, paragraph 37), in respect of which the Chief Ethics Commission is the controller, within the meaning of Article 2(d) of Directive 95/46 and Article 4(7) of the GDPR (see, by analogy, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 101).   
66      That having been explained, it should be examined whether Article 7 of Directive 95/46 and Article 6 of the GDPR, read in the light of Articles 7 and 8 of the Charter, preclude publication on the internet of part of the personal data set out in the declaration of private interests that any head of an establishment receiving public funds is required to lodge, such as the publication provided for in Article 10 of the Law on the reconciliation of interests.  
67      Article 7 of Directive 95/46 and the first subparagraph of Article 6(1) of the GDPR set out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being regarded as such, processing must fall within one of the cases provided for in those provisions (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 99 and the case-law cited).  
68      Under Article 7(e) of Directive 95/46 and point (e) of the first subparagraph of Article 6(1) of the GDPR, which are mentioned by the referring court in its first question, processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller is lawful. In addition, under Article 7(c) of that directive and under point (c) of the first subparagraph of Article 6(1) of that regulation, a provision to which that court referred in the grounds of its request for a preliminary ruling, processing that is necessary for compliance with a legal obligation to which the controller is subject is also lawful.   
69      Article 6(3) of the GDPR specifies, in respect of those two situations where processing is lawful, that the processing must be based on EU law or on Member State law to which the controller is subject, and that that legal basis must meet an objective of public interest and be proportionate to the legitimate aim pursued. Since those requirements constitute an expression of the requirements arising from Article 52(1) of the Charter, they must be interpreted in the light of the latter provision and must apply   
mutatis mutandis   
 to Article 7(c) and (e) of Directive 95/46.  
70      It should indeed be borne in mind that the fundamental rights to respect for private life and to the protection of personal data, guaranteed in Articles 7 and 8 of the Charter, are not absolute rights, but must be considered in relation to their function in society and be weighed against other fundamental rights. Limitations may therefore be imposed, so long as, in accordance with Article 52(1) of the Charter, they are provided for by law, respect the essence of the fundamental rights and observe the principle of proportionality. Under the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. They must apply only in so far as is strictly necessary and the legislation which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 105 and the case-law cited).  
71      In the present instance, given that the publication, on the Chief Ethics Commission’s website, of part of the personal data set out in the declaration of private interests that any head of an establishment receiving public funds is required to lodge results from a legislative provision of the Member State law to which the Chief Ethics Commission is subject, that is to say, from Article 10 of the Law on the reconciliation of interests, that processing is necessary for compliance with a legal obligation which is binding on that authority as controller and, therefore, falls within the situation envisaged in Article 7(c) of Directive 95/46 and point (c) of the first subparagraph of Article 6(1) of the GDPR. That being so, it is not necessary to determine whether that processing also falls within the situation envisaged in Article 7(e) of that directive and point (e) of the first subparagraph of Article 6(1) of that regulation.   
72      Furthermore, since, as is apparent from paragraph 63 of the present judgment, Article 10 of the Law on the reconciliation of interests defines the scope of the limitation on the exercise of the right to the protection of personal data, the interference that it entails must be regarded as provided for by law, within the meaning of Article 52(1) of the Charter (see, to that effect, judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 54).  
73      However, as has been stated in paragraph 69 of the present judgment, Article 10 of the Law on the reconciliation of interests, as the legal basis for the processing at issue in the main proceedings, must also fulfil the other requirements arising from Article 52(1) of the Charter and Article 6(3) of the GDPR, and in particular must meet an objective of public interest and be proportionate to the legitimate aim pursued.   
74      In the present instance, it is apparent from Article 1 of the Law on the reconciliation of interests that, in adopting the principle of transparency of declarations of interest, that law seeks to ensure that the public interest takes precedence when decisions are taken by persons working in the public service, to guarantee the impartiality of those decisions, and to prevent situations of conflict of interests and the emergence and spread of corruption in the public service.   
75      Such objectives, in that they seek to strengthen the safeguards for probity and impartiality of public sector decision makers, to prevent conflicts of interest and to combat corruption in the public sector, are undeniably objectives of public interest and, accordingly, legitimate.   
76      Indeed, ensuring that public sector decision makers perform their duties impartially and objectively and preventing them from being influenced by considerations relating to private interests have the aim of guaranteeing the proper management of public affairs and public property.  
77      Furthermore, combating corruption is an objective that the Member States have endorsed at both international and EU level.  
78      In particular, at EU level, the Member States have acceded to the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, under which each Member State is required to adopt the necessary measures to ensure that both active and passive corruption involving officials is a criminal offence.   
79      At international level, Article 1 of the United Nations Convention against Corruption states that the purposes of that convention are, inter alia, to promote and strengthen measures to prevent and combat corruption more efficiently and effectively, and to promote integrity, accountability and proper management of public affairs and public property. To that end, Article 7(4) of the convention provides that ‘each State Party shall, in accordance with the fundamental principles of its domestic law, endeavour to adopt, maintain and strengthen systems that promote transparency and prevent conflicts of interest’.  
80      It follows from the foregoing considerations that the processing of personal data pursuant to the Law on the reconciliation of interests is intended to meet objectives of general interest recognised by the European Union, within the meaning of Article 52(1) of the Charter, and objectives that are of public interest and therefore legitimate, within the meaning of Article 6(3) of the GDPR.  
81      Consequently, in accordance with those provisions, the objectives referred to in paragraphs 74 and 75 of the present judgment authorise limitations on the exercise of the rights guaranteed in Articles 7 and 8 of the Charter, provided in particular that the limitations genuinely meet those objectives and are proportionate to them.  
82      That being so, it must be ascertained whether the placing online, on the Chief Ethics Commission’s website, of part of the personal data contained in the declaration of private interests that any head of an establishment receiving public funds is required to lodge with that authority is appropriate for achieving the objectives of general interest defined in Article 1 of the Law on the reconciliation of interests and does not go beyond what is necessary in order to achieve those objectives (see, by analogy, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 109).  
83      So far as concerns, first of all, the question whether publication on the Chief Ethics Commission’s website of personal data contained in declarations of private interest is appropriate for achieving the objective of general interest defined in Article 1 of the Law on the reconciliation of interests, it should be pointed out that the placing online of some of the personal data contained in the declarations of private interests of public sector decision makers, in that it enables the existence of possible conflicts of interest liable to influence the performance of their duties to be revealed, is such as to induce them to act impartially. Thus, such implementation of the principle of transparency is capable of preventing conflicts of interest and corruption, of increasing the accountability of public sector actors and, therefore, of strengthening citizens’ trust in their actions.  
84      Accordingly, the measure at issue in the main proceedings appears appropriate for contributing to the achievement of the objectives of general interest that it pursues.  
85      As regards, next, the requirement of necessity, it is apparent from recital 39 of the GDPR that that requirement is met where the objective of general interest pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed in Articles 7 and 8 of the Charter, since derogations and limitations in relation to the principle of protection of such data must apply only in so far as is strictly necessary (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 110 and the case-law cited). Consequently, it should be ascertained in the present instance whether the objective of preventing conflicts of interest and corruption in the public sector by reinforcing the probity and impartiality of public officials might reasonably be achieved just as effectively by other measures less restrictive of the rights to respect for private life and to the protection of personal data of heads of establishments receiving public funds.  
86      That assessment must be carried out in the light of all the matters of fact and law specific to the Member State concerned – such as the existence of other measures designed to prevent conflicts of interest and combat corruption, and the scale of such conflicts and of the phenomenon of corruption within the public service – and of the nature of the information at issue and the importance of the duties carried out by the declarant, in particular his or her hierarchical position, the extent of the powers of public administration with which he or she may be vested and the powers that he or she has in relation to the commitment and management of public funds.  
87      In the present instance, first, it should be noted that, as can be gathered from paragraph 43 of the present judgment, the referring court seems to take the view that the obligation to declare private interests to the organs referred to in Articles 5 and 22 of the Law on the reconciliation of interests and the checking by those organs of compliance with that obligation and of the declaration’s content would enable the objectives pursued by that law, namely preventing conflicts of interest and combating corruption in the public sector, to be achieved just as effectively.  
88      According to the explanations provided by the referring court, one of the main arguments put forward by the Chief Ethics Commission in the main proceedings to justify publication of the declarations of private interest is the fact that it does not have sufficient human resources to check effectively all the declarations that are submitted to it.  
89      However, it must be pointed out that a lack of resources allocated to the public authorities cannot in any event constitute a legitimate ground justifying interference with the fundamental rights guaranteed by the Charter.  
90      The question also arises as to whether it is strictly necessary, in order to achieve the objectives of general interest referred to in Article 1 of the Law on the reconciliation of interests, that heads of establishments receiving public funds be, like the other categories of functions covered by the list in Article 10(1) of that law, subject to the public disclosure that that law prescribes.  
91      In that regard, the Lithuanian Government has stated before the Court that the obligation to provide a declaration of impartiality, to which those heads are subject under national law, is sufficient to achieve the objectives of the Law on the reconciliation of interests and that, therefore, application of Article 10 of that law to them, which was required until the Law on the reconciliation of interests as amended entered into force on 1 January 2020, went beyond what is strictly necessary in the light of those objectives.  
92      Second, even if publication of the private data at issue in the main proceedings were to prove necessary in order to achieve the objectives pursued by the Law on the reconciliation of interests, it is to be noted that a potentially unlimited number of persons may consult the personal data at issue. However, it is not apparent from the documents before the Court that the Lithuanian legislature, when adopting that provision, examined whether publication of those data on the internet without any restriction of access is strictly necessary or whether the objectives pursued by the Law on the reconciliation of interests might be achieved just as effectively if the number of persons able to consult those data is limited.  
93      Third, in any event, it is to be borne in mind that the condition relating to the necessity of processing must be examined in conjunction with the ‘data minimisation’ principle, enshrined in Article 6(1)(c) of Directive 95/46 and Article 5(1)(c) of the GDPR, under which personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (see, to that effect, judgment of 11 December 2019,   
Asociaţia de Proprietari bloc M5A  
-  
ScaraA  
, C-708/18, EU:C:2019:1064, paragraph 48).  
94      Therefore, only data the publication of which is actually capable of strengthening the safeguards for probity and impartiality of public officials, preventing conflicts of interest and combating corruption in the public sector may be subject to processing of the kind provided for in Article 10(1) of the Law on the reconciliation of interests.  
95      In the present instance, it is clear from Article 10(2) of the Law on the reconciliation of interests, and from the explanations provided by the referring court in response to the request by the Court for information, that the majority of the data that have to be set out in the declaration of private interests, pursuant to Article 6(1) of that law, are intended to be published on the Chief Ethics Commission’s website, with the exception, inter alia, of the data subjects’ personal identification number.  
96      Whilst, with a view to preventing conflicts of interest and corruption in the public sector, it may be appropriate to require information enabling the declarant to be identified and information relating to the activities of the declarant’s spouse, cohabitee or partner to be set out in the declarations of private interests, the public disclosure, online, of name-specific data relating to the spouse, cohabitee or partner of a head of an establishment receiving public funds, and to close relatives, or other persons known by the declarant, liable to give rise to a conflict of interests, seems to go beyond what is strictly necessary. As the Advocate General has observed in point 66 of his Opinion, it does not appear that the objectives of public interest pursued could not be achieved if, for the purposes of publication, reference were solely made generically to a spouse, cohabitee or partner, as the case may be, together with the relevant indication of the interests held by those persons in relation to their activities.  
97      Nor does it appear that the systematic publication, online, of the list of the declarant’s transactions the value of which is greater than EUR 3 000 is strictly necessary in the light of the objectives pursued.   
98      Finally, it must be borne in mind that an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 52). Consequently, for the purpose of assessing the proportionality of the processing at issue in the main proceedings, it is necessary to measure the seriousness of the interference with the fundamental rights to respect for private life and to the protection of personal data that that processing involves and to determine whether the importance of the objective of general interest pursued by the processing is proportionate to the seriousness of the interference.  
99      In order to assess the seriousness of that interference, account must be taken, inter alia, of the nature of the personal data at issue, in particular of any sensitivity of those data, and of the nature of, and specific methods for, the processing of the data at issue, in particular of the number of persons having access to those data and the methods of accessing them (judgment of 11 December 2019,   
Asociaţia de Proprietari bloc M5A  
-  
ScaraA  
, C-708/18, EU:C:2019:1064, paragraph 57).   
100    In the present instance, first, the public disclosure, online, of name-specific data relating to the declarant’s spouse, partner or cohabitee, or to persons who are close relatives of the declarant, or are known by him or her, liable to give rise to a conflict of interests, and mention of the subject of transactions the value of which is greater than EUR 3 000 are liable to reveal information on certain sensitive aspects of the data subjects’ private life, including, for example, their sexual orientation. Furthermore, since it envisages such public disclosure of name-specific data relating to persons other than the declarant in his or her capacity as a public sector decision maker, the processing of personal data that is provided for in Article 10 of the Law on the reconciliation of interests also concerns persons who do not have that capacity and in respect of whom the objectives pursued by that law are not imperative in the same way as for the declarant.  
101    The seriousness of such an infringement may still be increased by the cumulative effect of the personal data that are published as in the main proceedings, since combining them enables a particularly detailed picture of the data subjects’ private lives to be built up (see, to that effect, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 128).  
102    Second, it is not in dispute that that processing has the effect of making those personal data freely accessible on the internet to the whole of the general public and, accordingly, to a potentially unlimited number of persons.   
103    Consequently, that processing is liable to enable those data to be freely accessed by persons who, for reasons unrelated to the objective of general interest of preventing conflicts of interest and corruption in the public sector, seek to find out about the personal, material and financial situation of the declarant and the members of his or her family (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 118).   
104    Thus, as the Advocate General has observed in point 78 of his Opinion, publication of those data is liable, for example, to expose the persons concerned to repeated targeted advertising and commercial sales canvassing, or even to risks of criminal activity.  
105    Therefore, processing, such as that at issue in the main proceedings, of the personal data referred to in paragraph 100 of the present judgment must be regarded as constituting a serious interference with the fundamental rights of data subjects to respect for private life and to the protection of personal data.  
106    The seriousness of that interference must be weighed against the importance of the objectives of preventing conflicts of interest and corruption in the public sector.  
107    In that regard, the Court considers it useful, for the purpose of pointing out the importance within the European Union of the objective of combating corruption, to take into consideration the content of the report of the Commission to the Council and the European Parliament of 3 February 2014 entitled ‘EU Anti-Corruption Report’ (COM(2014) 38 final), according to which corruption – which impinges on good governance, sound management of public money, and competitive markets – hampers economic development, undermines democracy and damages social justice and the rule of law, and is capable of undermining the trust of citizens in democratic institutions and processes. The report states that the whole of the European Union is affected by that phenomenon, to a greater or lesser extent depending on the Member State.  
108    Similarly, the Criminal Law Convention on Corruption adopted by the Council of Europe refers to corruption in its fourth recital as a ‘[threat to] the rule of law, democracy and human rights [which] undermines good governance, fairness and social justice, distorts competition, hinders economic development and endangers the stability of democratic institutions and the moral foundations of society’.  
109    In the light of the foregoing, it is undeniable that combating corruption is of great importance within the European Union.  
110    In that context, the weighing of the interference resulting from the publication of personal data contained in the declarations of private interest against the objectives of general interest of preventing conflicts of interest and corruption in the public sector involves taking into consideration, inter alia, the fact and the extent of the phenomenon of corruption within the public service of the Member State concerned, so that the result of the weighing up to be carried out of those objectives, on the one hand, and a data subject’s rights to respect for private life and to the protection of personal data, on the other, is not necessarily the same for all the Member States (see, by analogy, judgment of 24 September 2019,   
Google (Territorial scope of de-referencing)  
, C-507/17, EU:C:2019:772, paragraph 67).  
111    Furthermore, as follows from paragraph 86 of the present judgment, for the purpose of that balancing exercise, account must be taken inter alia of the fact that the general interest in personal data being published may vary according to the importance of the duties carried out by the declarant, in particular his or her hierarchical position, the extent of the powers of public administration with which he or she may be vested and the powers that he or she has in relation to the commitment and management of public funds (see, by analogy, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 81).   
112    That having been explained, it must be found that the publication online of the majority of the personal data contained in the declaration of private interests of any head of an establishment receiving public funds, such as that at issue in the main proceedings, does not meet the requirements of a proper balance. In comparison with an obligation to declare coupled with a check of the declaration’s content by the Chief Ethics Commission the effectiveness of which it is for the Member State concerned to ensure by endowing that body with the means necessary for that purpose, such publication amounts to a considerably more serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, without that increased interference being capable of being offset by any benefits which might result from publication of all those data for the purpose of preventing conflicts of interest and combating corruption.  
113    Nor is there anything in the documents before the Court to indicate that safeguards against the risks of abuse, such as the risks referred to in paragraphs 103 and 104 of the present judgment, are provided for by the national legislation applicable to the dispute in the main proceedings.  
114    As regards, however, the data relating to the membership of the declarant – or, without being name-specific, to the membership of the declarant’s spouse, cohabitee or partner – of undertakings, establishments, associations or funds, to their activities as self-employed persons and to the legal persons of which they are members, it must be held that transparency as to whether or not such interests exist enables citizens and economic operators to have an accurate picture of the financial independence of the persons who are vested with decision-making power in the management of public funds. Furthermore, the data concerning gifts received, other than from close relatives, the value of which exceeds EUR 150 are capable of revealing the existence of acts of corruption.  
115    Subject to the requirement to strike a fair balance in the light of the extent of the declarant’s decision-making power, and provided that the principle of data minimisation is observed, the publication of such data contained in the declaration of interests may be justified by the benefits which, by strengthening the safeguards for probity and impartiality of public officials, such transparency brings in respect of the prevention of conflicts of interest and the combating of corruption.  
116    In the light of all the foregoing considerations, the answer to the first question is that Article 7(c) of Directive 95/46 and point (c) of the first subparagraph of Article 6(1) and Article 6(3) of the GDPR, read in the light of Articles 7, 8 and 52(1) of the Charter, must be interpreted as precluding national legislation that provides for the publication online of the declaration of private interests that any head of an establishment receiving public funds is required to lodge, in so far as, in particular, that publication concerns name-specific data relating to his or her spouse, cohabitee or partner, or to persons who are close relatives of the declarant, or are known by him or her, liable to give rise to a conflict of interests, or concerns any transaction concluded during the last 12 calendar months the value of which exceeds EUR 3 000.   
   
The   
second question  
117    By its second question, the referring court asks, in essence, whether Article 8(1) of Directive 95/46 and Article 9(1) of the GDPR must be interpreted as meaning that the publication, on the website of the public authority responsible for collecting and checking the content of declarations of private interests, of personal data that are liable to disclose indirectly the political opinions, trade union membership or sexual orientation of a natural person constitutes processing of special categories of personal data, for the purpose of those provisions.  
118    Article 8(1) of Directive 95/46 and Article 9(1) of the GDPR provide for the prohibition, inter alia, of processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of data concerning a natural person’s sex life or sexual orientation. According to the heading of those articles, these are special categories of personal data, and such data are also categorised as ‘sensitive data’ in recital 34 of that directive and recital 10 of that regulation.  
119    In the present instance, although the personal data the publication of which is mandatory pursuant to Article 10(1) of the Law on the reconciliation of interests are not, inherently, sensitive data for the purpose of Directive 95/46 and the GDPR, the referring court takes the view that it is possible to deduce from the name-specific data relating to the spouse, cohabitee or partner of the declarant certain information concerning the sex life or sexual orientation of the declarant and his or her spouse, cohabitee or partner.  
120    That being so, it should be determined whether data that are capable of revealing the sexual orientation of a natural person by means of an intellectual operation involving comparison or deduction fall within the special categories of personal data, for the purpose of Article 8(1) of Directive 95/46 and Article 9(1) of the GDPR.  
121    According to settled case-law, for the purpose of interpreting a provision of EU law it is necessary to consider not only its wording but also its context and the objectives of the legislation of which it forms part (judgment of 21 December 2021,   
Bank Melli Iran  
, C-124/20, EU:C:2021:1035, paragraph 43 and the case-law cited).  
122    Article 8(1) of Directive 95/46 states that Member States are to prohibit the processing of personal data ‘revealing’ racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data ‘concerning’ health or sex life. Article 9(1) of the GDPR provides that, inter alia, processing of personal data ‘revealing’ racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of data ‘concerning’ health or data ‘concerning’ a natural person’s sex life or sexual orientation, are to be prohibited.  
123    As the Advocate General has observed, in essence, in point 85 of his Opinion, whilst the use, in those provisions, of the verb ‘reveal’ is consistent with the taking into account of processing not only of inherently sensitive data, but also of data revealing information of that nature indirectly, following an intellectual operation involving deduction or cross-referencing, the preposition ‘concerning’ seems, on the other hand, to signify the existence of a more direct and immediate link between the processing and the data concerned, viewed inherently.  
124    Such an interpretation, which would result in a distinction being drawn according to the type of sensitive data at issue, would not, however, be consistent with a contextual analysis of those provisions, in particular with Article 4(15) of the GDPR, according to which ‘data concerning health’ are personal data related to the physical or mental health of a natural person, including the provision of health care services, which ‘reveal’ information about his or her health status, and with recital 35 of that regulation, which states that personal data concerning health should include all data pertaining to the health status of a data subject which ‘reveal’ information relating to the past, current or future physical or mental health status of the data subject.  
125    Furthermore, a wide interpretation of the terms ‘special categories of personal data’ and ‘sensitive data’ is confirmed by the objective of Directive 95/46 and the GDPR, noted in paragraph 61 of the present judgment, which is to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular of their private life, with respect to the processing of personal data concerning them (see, to that effect, judgment of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 50).  
126    The contrary interpretation would, moreover, run counter to the purpose of Article 8(1) of Directive 95/46 and Article 9(1) of the GDPR, namely to ensure enhanced protection as regards processing which, because of the particular sensitivity of the data processed, is liable to constitute, as follows from recital 33 of Directive 95/46 and recital 51 of the GDPR, a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 44).  
127    Consequently, those provisions cannot be interpreted as meaning that the processing of personal data that are liable indirectly to reveal sensitive information concerning a natural person is excluded from the strengthened protection regime prescribed by those provisions, if the effectiveness of that regime and the protection of the fundamental rights and freedoms of natural persons that it is intended to ensure are not to be compromised.  
128    In the light of all the foregoing considerations, the answer to the second question is that Article 8(1) of Directive 95/46 and Article 9(1) of the GDPR must be interpreted as meaning that the publication, on the website of the public authority responsible for collecting and checking the content of declarations of private interests, of personal data that are liable to disclose indirectly the sexual orientation of a natural person constitutes processing of special categories of personal data, for the purpose of those provisions.  
   
Costs  
129    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 7(c) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and point (c) of the first subparagraph of Article 6(1) and Article 6(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), read in the light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation that provides for the publication online of the declaration of private interests that any head of an establishment receiving public funds is required to lodge, in so far as, in particular, that publication concerns name-specific data relating to his or her spouse, cohabitee or partner, or to persons who are close relatives of the declarant, or are known by him or her, liable to give rise to a conflict of interests, or concerns any transaction concluded during the last 12 calendar months the value of which exceeds EUR 3 000.  
2.        
Article 8(1) of Directive 95/46 and Article 9(1) of Regulation 2016/679 must be interpreted as meaning that the publication, on the website of the public authority responsible for collecting and checking the content of declarations of private interests, of personal data that are liable to disclose indirectly the sexual orientation of a natural person constitutes processing of special categories of personal data, for the purpose of those provisions.

ID: 62d97b61-7129-4f4c-b91b-bf3bbdac9ff2

Judgment of 16 Dec 2008, C-73/07 (  
Satakunnan Markkinapörssi and Satamedia  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
General data protection law   
 >   
Chapter IX - Provisions relating to specific processing operations   
 >   
Processing and freedom of expression and information   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Household exemption   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
   
JUDGMENT OF THE COURT (Grand Chamber)  
16 December 2008 (\*)  
(Directive 95/46/EC – Scope – Processing and flow of tax data of a personal nature – Protection of natural persons – Freedom of expression)  
In Case C-73/07,  
REFERENCE for a preliminary ruling under Article 234 EC from the Korkein hallinto-oikeus (Finland), made by decision of 8 February 2007, received at the Court on 12 February 2007, in the proceedings  
Tietosuojavaltuutettu  
v  
Satakunnan Markkinapörssi Oy,  
Satamedia Oy,  
THE COURT (Grand Chamber),  
composed of V. Skouris, President, P. Jann, C.W.A. Timmermans, A. Rosas, K. Lenaerts and A. Ó Caoimh, Presidents of Chambers, P. Kūris, E. Juhász, G. Arestis, A. Borg Barthet, J. Klučka, U. Lõhmus and E. Levits (Rapporteur), Judges,  
Advocate General: J. Kokott,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 12 February 2008,  
after considering the observations submitted on behalf of:  
–        Satakunnan Markkinapörssi Oy and Satamedia Oy, by P. Vainio, asianajaja,  
–        the Finnish Government, by J. Heliskoski, acting as Agent,  
–        the Estonian Government, by L. Uibo, acting as Agent,  
–        the Portuguese Government, by L.I. Fernandes and C. Vieira Guerra, acting as Agents,  
–        the Swedish Government, by A. Falk and K. Petkovska, acting as Agents,  
–        the Commission of the European Communities, by C. Docksey and P. Aalto, acting as Agents,  
after hearing the Advocate General at the sitting on 8 May 2008,  
gives the following  
Judgment  
1        This reference for a preliminary ruling relates to the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) (‘the directive’).  
2        The reference was made in proceedings between the Tietosuojavaltuutettu (Data Protection Ombudsman) and the Tietosuojalautakunta (Data Protection Board) relating to activities involving the processing of personal data undertaken by Satakunnan Markkinapörssi Oy (‘Markkinapörssi’) and Satamedia Oy (‘Satamedia’).  
   
Legal context  
   
Community legislation   
3        As is apparent from Article 1(1) of the directive, its objective is to protect the fundamental rights and freedoms of natural persons, and, in particular, their right to privacy with respect to the processing of personal data.  
4        Article 1(2) of the directive states:  
‘Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
5        Article 2 of the directive, entitled ‘Definitions’, provides:  
‘For the purposes of this Directive:  
(a)       “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
(c)  
      “personal data filing system” (“filing system”) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;  
…’  
6        Article 3 of the directive defines its scope of application in the following manner:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
7        The relationship between the protection of personal data and freedom of expression is governed by Article 9 of the directive, entitled ‘Processing of personal data and freedom of expression’, in the following terms:  
‘Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.’  
8        In that connection, recital 37 in the preamble to the directive is worded as follows:  
‘Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of [expression] and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities.’   
9        Article 13 of the directive, entitled ‘Exemptions and restrictions’, states:  
‘1.      Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:  
(a)      national security;  
…’   
10      Article 17 of the directive, entitled ‘Security of processing’, provides:   
‘1.      Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.   
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.  
2.      The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.  
…’  
   
National legislation  
11      Paragraph 10(1) of the Constitution (Perustuslaki (731/1999)) of 11 June 1999 states:   
‘The right to privacy, honour and the inviolability of the home of every person shall be guaranteed. More detailed provisions on the protection of personal data shall be laid down by law.’  
12      Paragraph 12 of the Constitution provides:  
‘Everyone shall have the right to freedom of expression. Freedom of expression entails the right to express oneself and to disseminate and receive information, opinions and other communications without prior hindrance. More detailed provisions relating to the exercise of the right to freedom of expression shall be laid down by law. …’  
Documents and other records in the possession of the authorities shall be in the public domain, unless specifically restricted by law for compelling reasons. Every person shall have the right of access to public documents and records.’  
13      The Law on personal data (Henkilötietolaki (523/1999)) of 22 April 1999, which transposed the directive into national law, applies to the processing of those data (Paragraph 2(1)), apart from personal data files which contain solely, and in unaltered form, material that has been published in the media (Paragraph 2(4)). It applies only in part to the processing of personal data for journalistic purposes and for the purpose of artistic or literary expression (Paragraph 2(5)).   
14      Paragraph 32 of the Law on personal data provides that the controller is to take all technical and organisational measures necessary in order to protect personal data against unauthorised access to those data, and their accidental or unlawful destruction, alteration, disclosure or transfer, together with any other unlawful processing of those data.   
15      The Law on public access in relation to official activities (Laki viranomaisten toiminnan julkisuudesta (621/1999)) of 21 May 1999 also governs access to information.  
16      Paragraph 1(1) of the Law on public access in relation to official activities states that the general principle is that documents covered by that law are to be in the public domain.   
17      Paragraph 9 of that law provides that every person is to have the right of access to a public document held by the public authorities.   
18      Paragraph 16(1) of that law lays down the detailed rules governing access to a document of that kind. It provides that the public authorities are to explain the contents of the document orally, make the document available in their offices where it may be studied, copied or listened to, or issue a copy or a print-out of the document concerned.   
19      Paragraph 16(3) of that law specifies the circumstances in which data in files containing personal data kept by the public authorities may be disclosed:  
‘A file containing personal data may be disclosed in the form of a print-out, or those data may be disclosed in electronic form, unless provided otherwise by law, if the recipient is authorised to store and use such data by virtue of the provisions governing the protection of personal data. However, access to personal data for the purposes of direct marketing, market surveys or market research shall not be permitted unless specifically provided for by law or if the data subject has given his consent.’  
20      The national court states that the provisions of the Law on the public disclosure and confidentiality of tax information (Laki verotustietojen julkisuudesta ja salassapidosta (1346/1999)) of 30 December 1999 are to prevail over those of the Law on personal data and the Law on public access in relation to official activities.  
21      Paragraph 2 of the Law on the public disclosure and confidentiality of tax information provides that the provisions of the Law on public access in relation to official activities and the Law on personal data are to apply to documents and information relating to tax matters, save as may be otherwise provided in a legislative measure.   
22      Paragraph 3 of the Law on the public disclosure and confidentiality of tax information states:  
‘Information relating to tax matters shall be in the public domain in accordance with the detailed rules laid down in this law.   
Every person shall have the right to obtain access to a document relating to tax matters which is in the public domain and held by the tax authorities, in accordance with the detailed rules laid down in the Law on public access in relation to official activities, subject to the exceptions laid down in this law.’  
23      Paragraph 5(1) of the Law on the public disclosure and confidentiality of tax information provides that details of the taxpayer’s name, his date of birth and his municipality of residence, as set out in his annual tax return, are to be in the public domain. The following information is also in the public domain:  
‘1.      Earned income for the purposes of national taxation;  
2.      Unearned income and income from property for the purposes of national taxation;  
3.      Earned income for the purposes of municipal taxation;  
4.      Taxes on income and property, municipal taxes and the total amount of taxes and charges levied.  
…’  
24      Lastly, Paragraph 8 of Chapter 24 of the Criminal Code (Rikoslaki), in the version brought into force by Law 531/2000, imposes penalties in respect of the disclosure of information which infringes an individual’s right to privacy. Under those provisions, it is an offence to disseminate, through the media or otherwise, any information, innuendo or images relating to the private life of another person where to do so would be liable to cause harm or suffering to the person concerned or to bring that person into disrepute.   
   
The dispute in the main proceedings and the questions referred   
25      For several years, Markkinapörssi has collected public data from the Finnish tax authorities for the purposes of publishing extracts from those data in the regional editions of the   
Veropörssi   
newspaper each year.   
26      The information contained in those publications comprises the surname and given name of approximately 1.2 million natural persons whose income exceeds certain thresholds as well as the amount, to the nearest EUR 100, of their earned and unearned income and details relating to wealth tax levied on them. That information is set out in the form of an alphabetical list and organised according to municipality and income bracket.   
27      According to the order for reference, the   
Veropörssi   
newspaper carries a statement that the personal data disclosed may be removed on request and without charge.   
28      While that newspaper also contains articles, summaries and advertisements, its main purpose is to publish personal tax information.   
29      Markkinapörssi transferred personal data published in the   
Veropörssi  
 newspaper, in the form of CD-ROM discs, to Satamedia, which is owned by the same shareholders, with a view to those data being disseminated by a text-messaging system. In that connection, those companies signed an agreement with a mobile telephony company which put in place, on Satamedia’s behalf, a text-messaging service allowing mobile telephone users to receive information published in the   
Veropörssi   
newspaper on their telephone, for a charge of approximately EUR 2. Personal data are removed from that service on request.   
30      The Tietosuojavaltuutettu and the Tietosuojalautakunta, who are the Finnish authorities responsible for data protection, supervise the processing of personal data and have the regulatory powers laid down in the Law on personal data.   
31      Following complaints from individuals alleging infringement of their right to privacy, on 10 March 2004, the Tietosuojavaltuutettu responsible for investigating the activities of Markkinapörssi and Satamedia requested the Tietosuojalautakunta to prohibit the latter from carrying on the personal data processing activities at issue.  
32      That request having been rejected by the Tietosuojalautakunta, the Tietosuojavaltuutettu brought proceedings before the Helsingin hallinto-oikeus (Administrative Court, Helsinki), which also rejected his application. The Tietosuojavaltuutettu then brought an appeal before the Korkein hallinto-oikeus (Supreme Administrative Court).   
33      The national court emphasises that the appeal brought by the Tietosuojavaltuutettu does not concern the transfer of information by the Finnish authorities. It also states that the public nature of the tax data in question is not at issue. On the other hand, it has concerns as regards the subsequent processing of those data.  
34      In those circumstances, it decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:   
‘(1)  Can an activity in which data relating to the earned and unearned income and assets of natural persons are:  
(a)      collected from documents in the public domain held by the tax authorities and processed for publication,  
(b)      published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists,  
(c)      transferred onward on CD-ROM to be used for commercial purposes, and  
(d)      processed for the purposes of a text-messaging service whereby mobile telephone users can, by sending a text message containing details of an individual’s name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person,  
be regarded as the processing of personal data within the meaning of Article 3(1) of [the directive]?  
(2)      Is [the directive] to be interpreted as meaning that the various activities listed in Question 1(a) to (d) can be regarded as the processing of personal data carried out solely for journalistic purposes within the meaning of Article 9 of the directive, having regard to the fact that data on over one million taxpayers have been collected from information which is in the public domain under national legislation on the right of public access to information? Does the fact that publication of those data is the principal aim of the operation have any bearing on the assessment in this case?  
(3)      Is Article 17 of [the directive] to be interpreted in conjunction with the principles and purpose of the directive as precluding the publication of data collected for journalistic purposes and its onward transfer for commercial purposes?  
(4)      Is [the directive] to be interpreted as meaning that personal data files containing, solely and in unaltered form, material that has already been published in the media fall altogether outside its scope?’  
   
The questions referred  
   
The first question  
35      It must be held that the data to which this question relates, which comprise the surname and given name of certain natural persons whose income exceeds certain thresholds as well as the amount, to the nearest EUR 100, of their earned and unearned income, constitute personal data within the meaning of Article 2(a) of the directive, since they constitute ‘information relating to an identified or identifiable natural person’ (see also Joined Cases C-465/00, C-138/01 and C-139/01   
Österreichischer Rundfunk and Others   
[2003] ECR I-4989, paragraph 64).  
36      It is sufficient to hold, next, that it is clear from the wording itself of the definition set out in Article 2(b) of the directive that the activity to which the question relates involves the ‘processing of personal data’ within the meaning of that provision.  
37      Consequently, the answer to the first question must be that Article 3(1) of the directive is to be interpreted as meaning that an activity in which data on the earned and unearned income and the assets of natural persons are:  
–        collected from documents in the public domain held by the tax authorities and processed for publication,  
–        published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists,  
–        transferred onward on CD-ROM to be used for commercial purposes, and  
–        processed for the purposes of a text-messaging service whereby mobile telephone users can, by sending a text message containing details of an individual’s name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person,  
must be considered as the ‘processing of personal data’ within the meaning of that provision.   
   
The fourth question  
38      By its fourth question, which should be examined next, the national court asks, in essence, whether activities involving the processing of personal data such as those referred to at points (c) and (d) of the first question and relating to personal data files which contain solely, and in unaltered form, material that has already been published in the media, fall within the scope of application of the directive.  
39      By virtue of Article 3(2) of the directive, the directive does not apply to the processing of personal data in two situations.   
40      The first situation involves the processing of personal data undertaken in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and, in any case, to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.  
41      Those activities, which are mentioned by way of example in the first indent of Article 3(2) are, in any event, activities of the State or of State authorities unrelated to the fields of activity of individuals. They are intended to define the scope of the exception provided for there, with the result that that exception applies only to the activities which are expressly listed there or which can be classified in the same category (  
ejusdem generis  
) (see Case C-101/01   
Lindqvist  
 [2003] ECR I-12971, paragraphs 43 and 44).  
42      Activities involving the processing of personal data of the kind referred to at points (c) and (d) of the first question concern the activities of private companies. Those activities do not fall in any way within a framework established by the public authorities that relates to public security. Consequently, such activities cannot be assimilated to those covered by Article 3(2) of the directive (see, to that effect, Joined Cases C-317/04 and C-318/04   
Parliament   
v   
Council   
[2006] ECR I-4721, paragraph 58).   
43      As regards the second situation, which is covered by the second indent of that provision, recital 12 in the preamble to the directive – relating to that exception – mentions as examples of data processing carried out by a natural person in the course of a purely personal or household activity, correspondence and the holding of records of addresses.  
44      It follows that the latter exception must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals (see   
Lindqvist  
, paragraph 47). That clearly does not apply to the activities of Markkinapörssi and Satamedia, the purpose of which is to make the data collected accessible to an unrestricted number of people.   
45      It must therefore be held that activities involving the processing of personal data of the kind referred to at points (c) and (d) of the first question are not covered by any of the situations referred to in Article 3(2) of the directive.  
46      Moreover, it should be pointed out that the directive does not lay down any further limitation of its scope of application.  
47      In that regard, the Advocate General observes at point 125 of her Opinion that Article 13 of the directive permits derogations from its provisions only in certain cases, which do not extend to the provisions of Article 3.  
48      Lastly, it must be held that a general derogation from the application of the directive in respect of published information would largely deprive the directive of its effect. It would be sufficient for the Member States to publish data in order for those data to cease to enjoy the protection afforded by the directive.  
49      The answer to the fourth question should therefore be that activities involving the processing of personal data such as those referred to at points (c) and (d) of the first question and relating to personal data files which contain solely, and in unaltered form, material that has already been published in the media, fall within the scope of application of the directive.   
   
The second question  
50      By its second question, the national court asks, in essence, whether Article 9 of the directive should be interpreted as meaning that the activities referred to at points (a) to (d) of the first question, relating to data from documents which are in the public domain under national legislation, must be considered as activities involving the processing of personal data carried out solely for journalistic purposes. The national court states that it seeks clarification as to whether the fact that the principal aim of those activities is the publication of the data in question is relevant to the determination of that issue.  
51      It must be observed, as a preliminary point, that, according to settled case-law, the provisions of a directive must be interpreted in the light of the aims pursued by the directive and the system it establishes (see, to that effect, Case C-265/07   
Caffaro  
 [2008] ECR I-0000, paragraph 14).  
52      In that regard, it is not in dispute that, as is apparent from Article 1 of the directive, its objective is that the Member States should, while permitting the free flow of personal data, protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy, with respect to the processing of personal data.  
53      That objective cannot, however, be pursued without having regard to the fact that those fundamental rights must, to some degree, be reconciled with the fundamental right to freedom of expression.  
54      Article 9 of the directive refers to such a reconciliation. As is apparent, in particular, from recital 37 in the preamble to the directive, the object of Article 9 is to reconcile two fundamental rights: the protection of privacy and freedom of expression. The obligation to do so lies on the Member States.  
55      In order to reconcile those two ‘fundamental rights’ for the purposes of the directive, the Member States are required to provide for a number of derogations or limitations in relation to the protection of data and, therefore, in relation to the fundamental right to privacy, specified in Chapters II, IV and VI of the directive. Those derogations must be made solely for journalistic purposes or the purpose of artistic or literary expression, which fall within the scope of the fundamental right to freedom of expression, in so far as it is apparent that they are necessary in order to reconcile the right to privacy with the rules governing freedom of expression.   
56      In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly. Secondly, and in order to achieve a balance between the two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in the chapters of the directive referred to above must apply only in so far as is strictly necessary.   
57      In that context, the following points are relevant.  
58      First, as the Advocate General pointed out at point 65 of her Opinion and as is apparent from the legislative history of the directive, the exemptions and derogations provided for in Article 9 of the directive apply not only to media undertakings but also to every person engaged in journalism.  
59      Secondly, the fact that the publication of data within the public domain is done for profit-making purposes does not, prima facie, preclude such publication being considered as an activity undertaken ‘solely for journalistic purposes’. As Markkinapörssi and Satamedia state in their observations and as the Advocate General noted at point 82 of her Opinion, every undertaking will seek to generate a profit from its activities. A degree of commercial success may even be essential to professional journalistic activity.  
60      Thirdly, account must be taken of the evolution and proliferation of methods of communication and the dissemination of information. As was mentioned by the Swedish Government in particular, the medium which is used to transmit the processed data, whether it be classic in nature, such as paper or radio waves, or electronic, such as the internet, is not determinative as to whether an activity is undertaken ‘solely for journalistic purposes’.   
61      It follows from all of the above that activities such as those involved in the main proceedings, relating to data from documents which are in the public domain under national legislation, may be classified as ‘journalistic activities’ if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit-making purposes.  
62      The answer to the second question should therefore be that Article 9 of the directive is to be interpreted as meaning that the activities referred to at points (a) to (d) of the first question, relating to data from documents which are in the public domain under national legislation, must be considered as activities involving the processing of personal data carried out ‘solely for journalistic purposes’, within the meaning of that provision, if the sole object of those activities is the disclosure to the public of information, opinions or ideas. Whether that is the case is a matter for the national court to determine.  
The third question  
63      By its third question, the national court asks, in essence, whether Article 17 of the directive should be interpreted as meaning that it precludes the publication of data which have been collected for journalistic purposes and their onward transfer for commercial purposes.  
64      Having regard to the answer given to the second question, there is no need to reply to this question.   
   
Costs  
65      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is to be interpreted as meaning that an activity in which data on the earned and unearned income and the assets of natural persons are:  
–          
collected from documents in the public domain held by the tax authorities and processed for publication,  
–          
published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists,  
–          
transferred onward on CD-ROM to be used for commercial purposes, and   
–          
processed for the purposes of a text-messaging service whereby mobile telephone users can, by sending a text message containing details of an individual’s name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person,   
must be considered as the ‘processing of personal data’ within the meaning of that provision.  
2.        
Article 9 of Directive 95/46 is to be interpreted as meaning that the activities referred to at points (a) to (d) of the first question, relating to data from documents which are in the public domain under national legislation, must be considered as activities involving the processing of personal data carried out ‘solely for journalistic purposes’, within the meaning of that provision, if the sole object of those activities is the disclosure to the public of information, opinions or ideas. Whether that is the case is a matter for the national court to determine.   
3.        
Activities involving the processing of personal data such as those referred to at points (c) and (d) of the first question and relating to personal data files which contain solely, and in unaltered form, material that has already been published in the media, fall within the scope of application of Directive 95/46.

ID: 69ecff59-c059-4ad5-8d45-10b0b699058f

of 7 Dec 2023, C-634/21 (  
SCHUFA Holding and Others  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Automated individual decision-making, including profiling   
   
JUDGMENT OF THE COURT (First Chamber)  
7 December 2023 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 22 – Automated individual decision-making – Credit information agencies – Automated establishment of a probability value concerning the ability of a person to meet payment commitments in the future (‘scoring’) – Use of that probability value by third parties)  
In Case C-634/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), made by decision of 1 October 2021, received at the Court on 15 October 2021, in the proceedings  
OQ  
v  
Land Hessen,  
intervener:  
SCHUFA Holding AG,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, T. von Danwitz, P.G. Xuereb, A. Kumin (Rapporteur) and I. Ziemele, Judges,  
Advocate General: P. Pikamäe,  
Registrar: C. Di Bella, Administrator,  
having regard to the written procedure and further to the hearing on 26 January 2023,  
after considering the observations submitted on behalf of:  
–        OQ, by U. Schmidt, Rechtsanwalt,  
–        the Land Hessen, by M. Kottmann and G. Ziegenhorn, Rechtsanwälte,  
–        SCHUFA Holding AG, by G. Thüsing and U. Wuermeling, Rechtsanwalt,  
–        the German Government, by P.-L. Krüger, acting as Agent,  
–        the Danish Government, by V. Pasternak Jørgensen, M. Søndahl Wolff and Y. Thyregod Kollberg, acting as Agents,  
–        the Portuguese Government, by P. Barros da Costa, I. Oliveira, J. Ramos and C. Vieira Guerra, acting as Agents,  
–        the Finnish Government, by M. Pere, acting as Agent,  
–        the European Commission, by A. Bouchagiar, F. Erlbacher and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 16 March 2023,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 6(1) and Article 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2; ‘the GDPR’).  
2        The request has been made in proceedings between OQ and the Land Hessen (Federal State of Hesse, Germany) concerning the refusal of the Hessischer Beauftragter für Datenschutz und Informationsfreiheit (Data Protection and Freedom of Information Commissioner for the Federal State of Hesse, Germany; ‘the HBDI’) to order SCHUFA Holding AG (‘SCHUFA’) to grant an application lodged by OQ seeking to access and erase personal data concerning her.  
   
Legal context  
   
European Union law  
3        Recital 71 of the GDPR provides:  
‘The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes “profiling” that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of [European] Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.  
In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.’  
4        Entitled ‘Definitions’, Article 4 of that regulation provides:  
‘For the purposes of this Regulation:  
…  
(4)      “profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;  
…’  
5        Entitled ‘Principles relating to processing of personal data’, Article 5 of that regulation provides:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; … (“purpose limitation”);  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
(d)      accurate and, where necessary, kept up to date; … (“accuracy”);  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; … (“storage limitation”);  
(f)      processed in a manner that ensures appropriate security of the personal data … (“integrity and confidentiality”);  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
6        Entitled ‘Lawfulness of processing’, Article 6 of the GDPR provides, in paragraphs 1 and 3 thereof:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
(d)      processing is necessary in order to protect the vital interests of the data subject or of another natural person;  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
…  
3.      The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.  
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. …’  
7        Entitled ‘Processing of special categories of personal data’, Article 9 of that regulation is worded as follows:  
‘1.      Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.  
2.      Paragraph 1 shall not apply if one of the following applies:  
(a)      the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;  
…  
(g)      processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;  
…’  
8        Entitled ‘Information to be provided where personal data are collected from the data subject’, Article 13 of that regulation provides, in paragraph 2 thereof:   
‘In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:  
…  
(f)      the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.’  
9        Entitled ‘Information to be provided where personal data have not been obtained from the data subject’, Article 14 of the GDPR provides, in paragraph 2 thereof:   
‘In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:  
…  
(g)      the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.’  
10      Entitled ‘Right of access by the data subject’, Article 15 of that regulation provides, in paragraph 1 thereof:  
‘The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:  
…  
(h)      the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.’  
11      Entitled ‘Automated individual decision-making, including profiling’, Article 22 of that regulation provides:  
‘1.      The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.  
2.      Paragraph 1 shall not apply if the decision:  
(a)      is necessary for entering into, or performance of, a contract between the data subject and a data controller;  
(b)      is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or  
(c)      is based on the data subject’s explicit consent.  
3.      In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.  
4.      Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.’  
12      Entitled ‘Right to an effective judicial remedy against a supervisory authority’, Article 78 of the GDPR provides, in paragraph 1 thereof:  
‘Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.’  
   
German law  
13      Entitled ‘Protection of trade and commerce in the context of “scoring” and credit reports’, Paragraph 31 of the Bundesdatenschutzgesetz (Federal Law on data protection) of 30 June 2017 (BGBl. I, p. 2097; ‘the BDSG’), reads as follows:  
‘(1)      The use of a probability value regarding specific future behaviour of a natural person for the purpose of deciding on the establishment, implementation or termination of a contractual relationship with that person (“scoring”) shall be permissible only if  
1.      the provisions of data protection law have been complied with,  
2.      the data used to calculate the probability value are demonstrably relevant to the calculation of the probability of the specific behaviour, on the basis of a scientifically recognised mathematical statistical method,  
3.      the data used for the calculation of the probability value were not exclusively address data, and  
4.      where address data are used, the data subject has been notified of the intended use of such data before the calculation of the probability value; the notification must be documented.  
(2)      The use of a probability value determined by credit information agencies in relation to a natural person’s ability and willingness to pay shall, in the case where information about claims against that person is taken into account, be permissible only if the conditions under subparagraph 1 are met and claims relating to a performance owed but not rendered despite falling due are taken into account only if they are claims  
1.      which have been established by a judgment which has become final or has been declared provisionally enforceable or for which there is a debt instrument pursuant to Paragraph 794 of the Zivilprozessordnung [(Code of Civil Procedure)],  
2.      which have been established in accordance with Paragraph 178 of the Insolvenzordnung [(Insolvency Code)] and not contested by the debtor at the meeting for verification of claims,  
3.      which the debtor has expressly acknowledged,  
4.      in respect of which  
(a)      the debtor has been given formal notice in writing at least twice after the claim fell due,  
(b)      the first formal notice was given at least four weeks previously,  
(c)      the debtor has been informed in advance, but at the earliest at the time of the first formal notice, of the possibility that the claim might be taken into account by a credit information agency and  
(d)      the debtor has not contested the claim, or  
5.      whose underlying contractual relationship may be terminated without notice on the ground of arrears in payment and in respect of which the debtor has been informed in advance of the possibility that account might be taken of them by a credit information agency.  
The permissibility of the processing, including the determination of probability values and of other data relevant to creditworthiness, under general data protection law remains unaffected.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
14      SCHUFA is a private company under German law which provides its contractual partners with information on the creditworthiness of third parties, in particular, consumers. To that end, it establishes a prognosis on the probability of a future behaviour of a person (‘score’), such as the repayment of a loan, based on certain characteristics of that person, on the basis of mathematical and statistical procedures. The establishment of scores (‘scoring’) is based on the assumption that, by assigning a person to a group of other persons with comparable characteristics who have behaved in a certain way, similar behaviour can be predicted.  
15      It is apparent from the request for a preliminary ruling that OQ was refused the granting of a loan by a third party after having been the subject of negative information established by SCHUFA and transmitted to that third party. OQ applied for SCHUFA to send her information on the personal data registered and to erase some of the data which was allegedly incorrect.  
16      In response to that request, SCHUFA informed OQ of her score and outlined, in broad terms, the methods for calculating the scores. However, referring to trade secrecy, it refused to disclose the various elements taken into account for the purposes of that calculation and their weighting. Lastly, SCHUFA stated that it limited itself to sending information to its contractual partners and it was those contractual partners which made the actual contractual decisions.  
17      By a complaint lodged on 18 October 2018, OQ asked the HBDI, the competent supervisory authority, to order SCHUFA to grant her request for access to information and erasure.  
18      By decision of 3 June 2020, the HBDI rejected that application for an order, explaining that it was not established that SCHUFA did not comply with the requirements set out in Article 31 of the BDSG incumbent upon it with regard to its activity.  
19      OQ appealed against that decision before the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), the referring court, in accordance with Article 78(1) of the GDPR.  
20      According to that court, it is important to determine, for the purposes of ruling on the dispute before it, whether the establishment of a probability value such as that at issue in the main proceedings constitutes automated individual decision-making within the meaning of Article 22(1) of the GDPR. If that question is answered in the affirmative, the lawfulness of that activity would be subject, under Article 22(2)(b) of that regulation, to the condition that that decision be authorised by EU law or Member State law to which the controller is subject.   
21      In that regard, the referring court has doubts as to the argument that Article 22(1) of the GDPR is not applicable to the activity of companies such as SCHUFA. It bases its doubts, from a factual point of view, on the importance of a probability value such as that at issue in the main proceedings for the decision-making practice of third parties to which that probability value is transmitted and, from a legal point of view, mainly on the objectives pursued by that Article 22(1), and on the guarantees of legal protection enshrined by the GDPR.  
22      More specifically, the referring court notes that it is the probability value which normally determines whether and how the third party will contract with the person concerned. Article 22 of the GDPR precisely aims to protect people against the risks linked to decisions purely based on automation.  
23      By contrast, if Article 22(1) of the GDPR were to be interpreted as meaning that the status of ‘automated individual decision-making’ cannot be recognised, in a situation such as that at issue in the main proceedings, until the decision taken by the third party with regard to the data subject, this would result in a lacuna in legal protection. First, a company such as SCHUFA would not be required to provide access to the additional information to which the data subject is entitled under Article 15(1)(h) of that regulation because that company would not be the company which adopts ‘automated decision-making’ within the meaning of that provision and, consequently, within the meaning of Article 22(1) of that regulation. Secondly, the third party to whom the probability value is communicated could not provide that additional information because it does not have it.  
24      Thus, according to the referring court, to avoid such a lacuna in legal protection, it would be necessary for the establishment of a probability value such as that at issue in the main proceedings to fall within the scope of application of Article 22(1) of the GDPR.  
25      If such an interpretation were to be accepted, the lawfulness of that activity would then be subject to the existence of a legal basis at the level of the Member State concerned, under Article 22(2)(b) of that regulation. In the present case, while it is true that Article 31 of the BDSG may constitute such a legal basis in Germany, there are serious doubts as to the compatibility of that provision with Article 22 of the GDPR because the German legislature regulates only the ‘use’ of a probability value such as that at issue in the main proceedings, and not the establishment in itself of that value.  
26      By contrast, if the establishment of such a probability value does not constitute automated individual decision-making within the meaning of Article 22 of the GDPR, the opening clause appearing in paragraph 2(b) of that Article 22 would also not apply to national regulations regarding that activity. In view of the exhaustive, in principle, nature of the GDPR and in the absence of any other normative competence for such national regulations, it seems that the German legislature, by subjecting the establishment of probability values to more advanced conditions of substantive lawfulness, specifies the regulated matter by going beyond the requirements set out in Articles 6 and 22 of the GDPR, without having regulatory power for this purpose. If this point of view were to be correct, this would modify the margin of examination of the national supervisory authority, which would then have to assess the compatibility of the activity of credit information agencies in the light of Article 6 of that regulation.  
27      In those circumstances the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 22(1) of the [GDPR] to be interpreted as meaning that the automated establishment of a probability value concerning the ability of a data subject to service a loan in the future already constitutes a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her, where that value, determined by means of personal data of the data subject, is transmitted by the controller to a third-party controller and the latter draws strongly on that value for its decision on the establishment, implementation or termination of a contractual relationship with the data subject?  
(2)      If the first question is answered in the negative:  
are Articles 6(1) and 22 of the [GDPR] to be interpreted as precluding national legislation under which the use of a probability value – in the present case, in relation to a natural person’s ability and willingness to pay, in the case where information about claims against that person is taken into account – regarding specific future behaviour of a natural person for the purpose of deciding on the establishment, implementation or termination of a contractual relationship with that person (scoring) is permissible only if certain further conditions, which are set out in more detail in the grounds of the request for a preliminary ruling, are met?’  
   
Admissibility of the request for a preliminary ruling  
28      SCHUFA challenges the admissibility of the request for a preliminary ruling by arguing, in the first place, that the referring court is not called upon to review the content of a decision on a complaint, adopted by a supervisory authority such as the HBDI, since the judicial remedy against such a decision, provided for in Article 78(1) of the GDPR, serves only to verify whether that authority has complied with the obligations incumbent upon it under that regulation, in particular that of processing complaints, it being specified that that authority has discretion to decide whether and how it should act.  
29      In the second place, SCHUFA maintains that the referring court does not set out the specific reasons why the questions referred would be decisive for the resolution of the dispute in the main proceedings. The purpose of the latter would be a request for information on an actual score and the erasure of that score. In the present case, SCHUFA has sufficiently complied with its information obligation and has already erased the score subject to the procedure.  
30      In that regard, it should be borne in mind that, according to settled case-law of the Court, it is solely for the national court hearing the case, which must assume responsibility for the subsequent judicial decision, to determine, with regard to the particular aspects of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it refers to the Court. Consequently, where the questions submitted concern the interpretation of a rule of EU law, the Court is in principle bound to give a ruling (judgment of 12 January 2023,   
DOBELES HES  
, C-702/20 and C-17/21, EU:C:2023:1, paragraph 46 and the case-law cited).  
31      Accordingly, questions concerning EU law enjoy a presumption of relevance. The Court may refuse to give a ruling on a question referred by a national court only where it is quite obvious that the interpretation of a rule of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 12 January 2023,   
DOBELES HES  
, C-702/20 and C-17/21, EU:C:2023:1, paragraph 47 and the case-law cited).  
32      As regards, in the first place, the plea of inadmissibility based on an allegedly limited judicial review to which decisions on complaints adopted by a supervisory authority are subject, it should be borne in mind that, under Article 78(1) of the GDPR, without prejudice to any other administrative or non-judicial remedy, each natural or legal person is to have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.  
33      In the present case, the decision adopted by the HBDI as supervisory authority constitutes a legally binding decision, within the meaning of Article 78(1) of the GDPR. Having examined the merits of the complaint brought before it, that authority ruled on it and found that the processing of personal data contested by the applicant in the main proceedings was lawful.   
34      With regard to the extent of the judicial review exercised over such a decision in the context of an action brought under Article 78(1), it is sufficient to note that a decision on a complaint adopted by a supervisory authority is subject to full judicial review (judgment of 7 December 2023,   
SCHUFA Holding (Discharge from remaining debts)  
, C-26/22 and C-64/22, EU:C:2023:XXX, point 1 of the operative part).  
35      The first plea of inadmissibility put forward by SCHUFA must therefore be rejected.  
36      In the second place, it is clear from the request for a preliminary ruling that the referring court questions the criterion of review to be used when assessing, in the light of the GDPR, the processing of the personal data at issue in the main proceedings, that criterion depending on the applicability or not of Article 22(1) of that regulation.  
37      Thus, it is not clear that the interpretation of the GDPR sought by the referring court bears no relation to the actual facts of the main action or its purpose and that the problem is hypothetical. Furthermore, the Court has before it the factual or legal material necessary to give a useful answer to the questions submitted to it.  
38      Accordingly, the second plea of inadmissibility put forward by SCHUFA must also be rejected.  
39      In those circumstances, the request for a preliminary ruling is admissible.  
   
Consideration of the questions referred  
   
The first question  
40      By its first question, the referring court asks, in essence, whether Article 22(1) of the GDPR must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes ‘automated individual decision-making’ within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person.  
41      In order to answer that question, it should be borne in mind, as a preliminary point, that the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 22 June 2023,   
Pankki S  
, C-579/21, EU:C:2023:501, paragraph 38 and the case-law cited).  
42      As regards the wording of Article 22(1) of the GDPR, that provision provides that the data subject is to have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.  
43      The applicability of that provision is therefore subject to three cumulative conditions, namely, first, that there must be a ‘decision’, secondly, that that decision must be ‘based solely on automated processing, including profiling’, and, thirdly, that it must produce ‘legal effects concerning [the interested party]’ or ‘similarly significantly [affect] him or her’.  
44      As regards, first, the condition relating to the existence of a decision, it should be noted that the concept of ‘decision’, within the meaning of Article 22(1) of the GDPR, is not defined by that regulation. However, it is apparent from the very wording of that provision that that concept refers not only to acts which produce legal effects concerning the person at issue but also to acts which similarly significantly affect him or her.  
45      The broad scope of the concept of ‘decision’ is confirmed by recital 71 of the GDPR, according to which a decision evaluating personal aspects relating to a person, to which that person should have the right not to be subject, ‘may include a measure’ which either produces ‘legal effects concerning him or her’, or, ‘similarly significantly affects him or her’. Under that recital, the term ‘decision’ covers, for example, the automatic refusal of an online credit application or e-recruiting practices without human intervention.  
46      The concept of ‘decision’ within the meaning of Article 22(1) of the GDPR is thus, as the Advocate General noted in point 38 of his Opinion, capable of including a number of acts which may affect the data subject in many ways, since that concept is broad enough to encompass the result of calculating a person’s creditworthiness in the form of a probability value concerning that person’s ability to meet payment commitments in the future.  
47      As regards, secondly, the condition according to which the decision, within the meaning of that Article 22(1), must be ‘based solely on automated processing, including profiling’, as the Advocate General noted in point 33 of his Opinion, it is common ground that an activity such as that of SCHUFA meets the definition of ‘profiling’ appearing in Article 4(4) of the GDPR and therefore that that condition is met in the present case, since the wording of the first question referred explicitly refers to the automated establishment of a probability value based on personal data relating to a person and concerning that person’s ability to repay a loan in the future.  
48      As regards, thirdly, the condition that the decision must produce ‘legal effects’ concerning the person at issue or affect him or her ‘similarly significantly’, it is apparent from the very wording of the first question referred that the action of the third party to whom the probability value is transmitted draws ‘strongly’ on that value. Thus, according to the factual findings of the referring court, in the event where a loan application is sent by a consumer to a bank, an insufficient probability value leads, in almost all cases, to the refusal of that bank to grant the loan applied for.  
49      In those circumstances, it must be stated that the third condition to which the application of Article 22(1) of the GDPR is subject is also fulfilled, since a probability value such as that at issue in the main proceedings affects, at the very least, the data subject significantly.  
50      It follows that, in circumstances such as those at issue in the main proceedings, in which the probability value established by a credit information agency and communicated to a bank plays a determining role in the granting of credit, the establishment of that value must be qualified in itself as a decision producing vis-à-vis a data subject ‘legal effects concerning him or her or similarly significantly [affecting] him or her’ within the meaning of Article 22(1) of the GDPR.  
51      That interpretation is corroborated by the context in which Article 22(1) of the GDPR takes place and by the objectives and purpose pursued by that regulation.  
52      In this regard, it is important to note that, as the Advocate General observed in point 31 of his Opinion, Article 22(1) of the GDPR confers on the data subject the ‘right’ not to be the subject of a decision solely based on automated processing, including profiling. That provision lays down a prohibition in principle, the infringement of which does not need to be invoked individually by such a person.  
53      As follows from a combined reading of Article 22(2) of the GDPR and recital 71 of that regulation, the adoption of a decision based solely on automated processing is authorised only in the cases referred to in that Article 22(2), namely where that decision is necessary for entering into, or performance of, a contract between the data subject and a data controller (point (a)), where it is authorised by EU or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests (point (b)), or where it is based on the data subject’s explicit consent (point (c)).  
54      Furthermore, Article 22 of the GDPR provides, in paragraphs 2(b) and 3 thereof, that suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests must be taken. In the cases referred to in points (a) and (c) of Article 22(2) of that regulation, the data controller is to implement at least the right of the data subject to obtain human intervention, to express his or her point of view and to contest the decision.  
55      In addition, under Article 22(4) of the GDPR, it is only in certain specific cases that automated individual decision-making within the meaning of Article 22 are to be based on special categories of personal data referred to in Article 9(1) of that regulation.  
56      Furthermore, in the case of automated decision-making, such as that referred to in Article 22(1) of the GDPR, first, the controller is subject to additional information obligations under Article 13(2)(f) and Article 14(2)(g) of that regulation. Secondly, the data subject enjoys, under Article 15(1)(h) of that regulation, the right to obtain from the controller, in particular, ‘meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject’.  
57      Those enhanced requirements as to the lawfulness of automated decision-making and the additional information obligations of the controller and the related additional rights of access of the data subject are explained by the purpose pursued by Article 22 of the GDPR, consisting of protecting individuals against the particular risks to their rights and freedoms represented by the automated processing of personal data, including profiling.  
58      That processing involves, as is apparent from recital 71 of the GDPR, the evaluation of personal aspects relating to the natural person concerned by that processing, in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.  
59      Those particular risks are, under that recital, likely to weigh on the legitimate interests and rights of the data subject, in particular taking account of discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation. It is therefore important, still according to that recital, to provide suitable safeguards and to ensure fair and transparent processing in respect of the data subject, in particular through the use of appropriate mathematical or statistical procedures for the profiling and the implementation of technical and organisational measures appropriate to ensure that the risk of errors is minimised.  
60      The interpretation set out in paragraphs 42 to 50 of this judgment, and in particular the broad scope of the concept of ‘decision’ within the meaning of Article 22(1) of the GDPR, reinforces the effective protection intended by that provision.  
61      On the other hand, in circumstances such as those at issue in the main proceedings, in which three stakeholders are involved, there would be a risk of circumventing Article 22 of the GDPR and, consequently, a lacuna in legal protection if a restrictive interpretation of that provision was retained, according to which the establishment of the probability value must only be considered as a preparatory act and only the act adopted by the third party can, where appropriate, be classified as a ‘decision’ within the meaning of Article 22(1) of that regulation.  
62      In that situation, the establishment of a probability value such as that at issue in the main proceedings would escape the specific requirements provided for in Article 22(2) to (4) of the GDPR, even though that procedure is based on automated processing and that it produces effects significantly affecting the data subject to the extent that the action of the third party to whom that probability value is transmitted draws strongly on it.  
63      Furthermore, as the Advocate General noted in point 48 of his Opinion, first, the data subject would not be able to assert, from the credit information agency which establishes the probability value concerning him or her, his or her right of access to the specific information referred to in Article 15(1)(h) of the GDPR, in the absence of automated decision-making by that company. Secondly, even assuming that the act adopted by the third party falls within the scope of Article 22(1) of that regulation in so far as it fulfils the conditions for application of that provision, that third party would not be able to provide that specific information because it generally does not have it.  
64      The fact that the establishment of a probability value such as that at issue in the main proceedings is covered by Article 22(1) of the GDPR has the consequence, as noted in paragraphs 53 to 55 of this judgment, that it is prohibited unless one of the exceptions set out in Article 22(2) of that regulation is applicable and the specific requirements provided for in Article 22(3) and (4) of that regulation are complied with.   
65      With regard, more specifically, to Article 22(2)(b) of the GDPR, to which the referring court refers, it is apparent from the very wording of that provision that the national law which authorises the adoption of an automated individual decision must lay down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests.   
66      In the light of recital 71 of the GDPR, such measures must include, in particular, the obligation for the controller to use appropriate mathematical or statistical procedures, implement technical and organisational measures appropriate to ensure that the risk of errors is minimised and inaccuracies are corrected, and secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and prevent, inter alia, discriminatory effects on that person. Those measures include, moreover, at least the right for the data subject to obtain human intervention on the part of the controller, to express his or her point of view and to challenge the decision taken in his or her regard.  
67      It is also important to note that, in accordance with the settled case-law of the Court, any processing of personal data must, first, comply with the principles relating to the processing of data established in Article 5 of the GDPR and, secondly, in the light, in particular, of the principle of the lawfulness of processing, laid down in Article 5(1)(a), satisfy one of the conditions of the lawfulness of the processing listed in Article 6 of that regulation (judgment of 20 October 2022,   
Digi  
, C-77/21, EU:C:2022:805, paragraph 49 and the case-law cited). The controller must be able to demonstrate compliance with those principles, in accordance with the principle of accountability set out in Article 5(2) of that regulation (see, to that effect, judgment of 20 October 2022,   
Digi  
, C-77/21, EU:C:2022:805, paragraph 24).  
68      Thus, in the event that the law of a Member State authorises, under Article 22(2)(b) of the GDPR, the adoption of a decision solely based on automated processing, that processing must comply not only with the conditions set out in the latter provision and in Article 22(4) of that regulation, but also with the requirements set out in Articles 5 and 6 of that regulation. Accordingly, Member States cannot adopt, under Article 22(2)(b) of the GDPR, regulations which authorise profiling in disregard of the requirements laid down by those Articles 5 and 6, as interpreted by the case-law of the Court.  
69      With regard in particular to the conditions of lawfulness, provided for in Article 6(1)(a), (b), and (f) of the GDPR, which are likely to apply in a case such as that at issue in the main proceedings, Member States are not empowered to provide additional rules for the implementation of those conditions, such an option being, in accordance with Article 6(3) of that regulation, limited to the reasons referred to in Article 6(1)(c) and (e) of that regulation.  
70      Furthermore, with regard more specifically to Article 6(1)(f) of the GDPR, Member States cannot, under Article 22(2)(b) of that regulation, dismiss the requirements resulting from the case-law of the Court following the judgment of 7 December 2023,   
SCHUFA Holding (Discharge from remaining debts)  
 (C-26/22 and C-64/22, EU:C:2023:XXX), in particular, by definitively prescribing the result of the balancing of the rights and interests at issue (see, to that effect, judgment of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 62).  
71      In the present case, the referring court states that only Paragraph 31 of the BDSG could constitute a national legal basis for the purposes of Article 22(2)(b) of the GDPR. However, it has serious doubts as to the compatibility of Paragraph 31 of the BDSG with EU law. Assuming that that provision is deemed incompatible with EU law, SCHUFA would act not only without legal basis, but would   
ipso iure  
 disregard the prohibition laid down in Article 22(1) of the GDPR.  
72      In this regard, it is for the referring court to verify whether Paragraph 31 of the BDSG can be classified as a legal basis authorising, under Article 22(2)(b) of the GDPR, the adoption of a decision solely based on automated processing. If that court were to reach the conclusion that Article 31 of the GDPR constitutes such a legal basis, it would still be up to it to verify whether the conditions set out in Article 22(2)(b) and (4) of the GDPR and those laid down in Articles 5 and 6 of that regulation are fulfilled in this case.  
73      In the light of all the foregoing considerations, the answer to the first question is that Article 22(1) of the GDPR must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes ‘automated individual decision-making’ within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person.  
   
The second question  
74      Given the answer to the first question, there is no need to answer the second question.  
   
Costs  
75      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
Article 22(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes ‘automated individual decision-making’ within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person.

ID: 6ae2aa00-54ef-48ba-8b85-bda3f58c29d7

of 8 Dec 2022, C-460/20 (  
Google  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accuracy   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
   
JUDGMENT OF THE COURT (Grand Chamber)  
8 December 2022 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Directive 95/46/EC – Article 12(b) – Point (a) of the first paragraph of Article 14 – Regulation (EU) 2016/679 – Article 17(3)(a) – Operator of an internet search engine – Research carried out on the basis of a person’s name – Displaying a link to articles containing allegedly inaccurate information in the list of search results – Displaying, in the form of thumbnails, photographs illustrating those articles in the list of results of an image search – Request for de-referencing made to the operator of the search engine – Weighing-up of fundamental rights – Articles 7, 8, 11 and 16 of the Charter of Fundamental Rights of the European Union – Obligations and responsibilities of the operator of the search engine in respect of processing a request for de-referencing – Burden of proof on the person requesting de-referencing)  
In Case C-460/20,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 27 July 2020, received at the Court on 24 September 2020, in the proceedings  
TU,  
RE  
v  
Google LLC  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Prechal, K. Jürimäe, C. Lycourgos, P.G. Xuereb, L.S. Rossi and D. Gratsias, Presidents of Chambers, M. Ilešič (Rapporteur), F. Biltgen, N. Piçarra, N. Jääskinen, N. Wahl, I. Ziemele and J. Passer, Judges,  
Advocate General: G. Pitruzzella,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 24 January 2022,  
after considering the observations submitted on behalf of:  
–        TU and RE, by M. Siegmann and T. Stöber, Rechtsanwälte,  
–        Google LLC, by B. Heymann, J. Spiegel and J. Wimmers, Rechtsanwälte,  
–        the Greek Government, by S. Charitaki, A. Magrippi and M. Tassopoulou, acting as Agents,  
–        the Austrian Government, by G. Kunnert, A. Posch and J. Schmoll, acting as Agents,  
–        the Romanian Government, by E. Gane and L. Liţu, acting as Agents,  
–        the European Commission, by A. Bouchagiar, F. Erlbacher, H. Kranenborg and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 7 April 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 17(3)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’) and Article 12(b) and point (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L281, p.31), read in the light of Articles 7, 8, 11 and 16 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between TU and RE, of the one part, and Google LLC, of the other part, concerning a request seeking, first, that articles in which they are identified be de-referenced from the results of a search carried out on the basis of their names and, second, that photographs representing them, displayed in the form of preview images (‘thumbnails’), be removed from the results of an image search.  
   
Legal context  
   
Directive 95/46  
3        Article 1 of Directive 95/46, entitled ‘Object of the Directive’, provided in paragraph 1 thereof:  
‘In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.’  
4        Article 2 of that directive, entitled ‘Definitions’, provided:  
‘For the purposes of this Directive:  
(a) “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); …  
(b) “processing of personal data” (“processing”): shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, …  
(d) “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; …’  
5        In Section I of Chapter II of that directive, entitled ‘Principles relating to data quality’, Article 6 was worded as follows:  
‘1.      Member States shall provide that personal data must be:  
…  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;  
…’  
6        In Section V of Chapter II of that directive, entitled ‘The data subject’s right of access to data’, Article 12 thereof, itself entitled ‘Right of access’, stated:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
…  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
…’  
7        In Section VII of Chapter II of Directive 95/46, entitled ‘The data subject’s right to object’, the first paragraph of Article 14 of that directive provided:  
‘Member States shall grant the data subject the right:  
(a)      at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;  
…’  
   
The GDPR  
8        As provided in Article 94(1) thereof, the GDPR repealed Directive 95/46 with effect from 25 May 2018. By virtue of Article 99(2), the GDPR applies from that date.  
9        Recitals 4, 39 and 65 of that regulation state:  
‘4.      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.  
…  
39.      … Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. …  
65.      A data subject should have the right to have personal data concerning him or her rectified and a “right to be forgotten” where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. … However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information …’  
10      In Chapter I of that regulation, entitled ‘General provisions’, Article 4 thereof, itself entitled ‘Definitions’, is worded as follows:  
‘For the purposes of this Regulation:  
(1) “personal data” means any information relating to an identified or identifiable natural person (“data subject”); …  
(2) “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means …  
(7) “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …’  
11      In Chapter II of that regulation, entitled ‘Principles’, Article 5, itself entitled ‘Principles relating to the processing of personal data’, provides:  
‘1.      Personal data shall be:  
…  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);  
…  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
12      Section 3 of Chapter III of the GDPR, entitled ‘Rectification and erasure’, includes, inter alia, Articles 16 and 17 of that regulation.  
13      Article 16 of the GDPR, entitled ‘Right of rectification’, provides:  
‘The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.’  
14      Article 17 of that regulation, entitled ‘Right to erasure (“right to be forgotten”)’, is worded as follows:  
‘1.      The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:  
(a)      the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;  
(b)      the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;  
(c)      the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);  
(d)      the personal data have been unlawfully processed;  
(e)      the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;  
(f)      the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).  
2.      Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.  
3.      Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:  
(a)      for exercising the right of freedom of expression and information;  
…’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
15      TU is a member of the board of directors and the only shareholder of an investment company as well as chairman of a subsidiary of that company, which, together with other companies, constitute a group of companies. He is also the sole shareholder in a third company, which is the sole shareholder in a fourth company, which in turn holds 60% of the shares in a fifth company.  
16      RE was TU’s cohabiting partner and, until May 2015, held general commercial power of representation in that fourth company.  
17      On 27 April, 4 June and 16 June 2015, three articles which criticised the investment model implemented by the fifth company and the group of companies referred to in paragraph 15 of the present judgment were published on the website www.g …net (‘the g-net website’). The 4 June 2015 article was also illustrated by three photographs of TU driving a luxury car, in a helicopter and in front of an airplane, respectively, as well as a photograph of RE in a convertible car.  
18      The operator of the g-net website is, according to the imprint, G-LLC, whose registered office is in New York (United States). The corporate purpose of G-LLC is, according to its own statement, ‘to contribute consistently towards fraud prevention in the economy and society by means of active investigation and constant transparency’. Various publications criticised G-LLC’s business model, in particular accusing it of attempting to ‘blackmail’ companies by first publishing negative reports regarding those companies and then offering to delete them or prevent their publication, in exchange for a sum of money.  
19      Google displayed the articles of 4 June 2015 and 16 June 2015 when the names and forenames of the applicants in the main proceedings, both on their own and in conjunction with certain company names, were entered in its search engine, as well as the 27 April 2015 article when certain company names were entered, and included a link to those articles. In addition, when an image search was conducted on that search engine, Google displayed in the list of results, in the form of thumbnails, the photographs of the applicants in the main proceedings contained in the article of 4 June 2015. Those photographs ceased being displayed in September 2017, at the latest. The articles ceased to be accessible on the g-net website from 28 June 2018 at the latest.  
20      The applicants in the main proceedings requested Google, as the controller of personal data processed by its search engine, first, to de-reference the links to the articles at issue in the main proceedings from the list of search results, on the ground that they contained inaccurate claims and defamatory opinions, and, second, to remove the thumbnails from the list of search results. They also claimed to have been victims of ‘blackmail’ by G-LLC.  
21      Google refused to comply with that request, referring to the professional context in which the articles and photographs at issue in the main proceedings were set and arguing that it was unaware of the alleged inaccuracy of the information contained in those articles.  
22      In 2015, the applicants in the main proceedings brought an action before the Landgericht Köln (Regional Court, Cologne, Germany) seeking an order requiring Google to de-reference the links to the articles at issue in the main proceedings from its lists of search results and to put an end to the display, in the form of thumbnails, of the photographs representing them. By judgment of 22 November 2017, that court dismissed the action.  
23      The applicants in the main proceedings lodged an appeal against that judgment before the Oberlandesgericht Köln (Higher Regional Court, Cologne, Germany). That appeal was dismissed by judgment of 8 November 2018. That court stated that the specific method of functioning of a search engine and the particular importance it has for the functioning of the internet must be accorded particular importance in the context of the weighing-up of competing rights and interests which is to be undertaken. Given that the operator of the search engine generally has no legal relationship with those providing the content shown, and given that it is impossible for that operator to investigate the facts and assess them while also taking account of the opinions of those providers, the operator of the search engine is subject to specific obligations to act only when it becomes aware, following a specific notification from the data subject, of a prima facie flagrant and clearly discernible infringement of the law. Those principles also apply where the search engine is used solely to search for images, given that the relevant interests involved are comparable.  
24      The appeal court added that, in so far as it is necessary conclusively to take account of the accuracy of the alleged fact, the burden of proof in that regard lies with the person requesting the de-referencing. In the present case, since the applicants in the main proceedings have not proven that the facts reported in relation to them are inaccurate, Google is unable to carry out a final assessment of the articles at issue in the main proceedings and, consequently, is not required to de-reference them. As regards the photographs displayed in the form of thumbnails, they could, in so far as they accompany one of those articles, be regarded as being news images.  
25      The applicants in the main proceedings brought an appeal on a point of law before the Bundesgerichtshof (Federal Court of Justice, Germany), the referring court.  
26      That court observes that the outcome of that action depends on the interpretation of EU law, in particular Article 17(3)(a) of the GDPR and Article 12(b) and point (a) of the first paragraph of Article 14 of Directive 95/46.  
27      As a preliminary point, the referring court states that, from its point of view, the request that Google be ordered to de-reference the links to the articles at issue in the main proceedings from the list of search results falls ratione temporis within the scope of the GDPR, whereas the request that Google be ordered to remove the thumbnails from the list of results of an image search falls ratione temporis within the scope of Directive 95/46, given that those thumbnails were no longer displayed by the search engine operated by Google on the date when the GDPR entered into force. However, as regards the request to have the thumbnails removed, the referring court requests the Court to provide an answer on that point which also takes account of that regulation.  
28      The referring court then observes that the fact that the articles at issue in the main proceedings are no longer available on the g-net website and that Google no longer displays the thumbnails has not eliminated the interest the applicants in the main proceedings have in pursuing their request for de-referencing, given that the g-net website merely states that, for various reasons, those articles are ‘currently’ unavailable. In those circumstances, it cannot be ruled out that those articles may be re-posted online in the future and may once more be referenced by Google’s search engine, since it is noted, moreover, that Google continues to take the view that that request for de-referencing is unjustified and Google continues to refuse to accede to it.  
29      As regards the substance, concerning, in the first place, the request for de-referencing of the links to the articles at issue in the main proceedings from the list of search results, the referring court notes that the applicants in the main proceedings justify that request by claiming, in particular, that some of the assertions in those articles are inaccurate. The question therefore arises as to whether it was for the applicants in the main proceedings to prove the alleged inaccuracy of those assertions or, at the very least, to furnish a certain degree of evidence of that inaccuracy or whether, on the contrary, Google ought either to have presumed that the claims of the applicants in the main proceedings were accurate or to have sought to clarify the facts itself.  
30      According to the referring court, the requirement to strike an equal balance between competing fundamental rights arising from Articles 7 and 8 of the Charter, on the one hand, and Articles 11 and 16 of the Charter, on the other, is not satisfied if, in a situation such as that at issue in the case in the main proceedings, the burden of proof falls exclusively on one party or the other.  
31      Consequently, that court proposes adopting a solution which seeks to require the data subject to resolve, at least provisionally, the question of the accuracy of the referenced content by pursuing in court his or her claim against the content provider, in so far as obtaining judicial protection at least provisionally is a reasonable option for the data subject taking account of the circumstances of the particular case. It is true that, in so far as it has no relationship with the content provider, the data subject could encounter the same difficulties as the operator of the search in making contact with the content provider. However, the data subject knows whether the referenced content is accurate or not. The question whether that data subject may reasonably be required to pursue in court his or her claim against the content supplier could depend, for example, on whether or not the content provider can be approached without particular difficulty within the European Union.  
32      Accordingly, the referring court suggests that, as a general rule, the data subject may reasonably be required to bring an action for interim relief against a content supplier whose name is known, but not against an anonymous provider or a provider to whom it is impossible to make notifications. However, the actual likelihood of obtaining enforcement of any order against the content provider requiring erasure is irrelevant as regards the rights vis-à-vis the operator of the search engine.  
33      In the second place, as regards the request that Google be ordered to put an end to the display, in the form of thumbnails, of the photographs of the applicants in the main proceedings contained in the 4 June 2015 article, the referring court observes, first of all, that those thumbnails do indeed contain a link allowing access to the third party’s internet page on which the corresponding photograph was published and thereby to become aware of the context of that publication. However, in so far as the list of results of an image search displays only thumbnails, without reproducing information regarding the context of that publication on the third party’s internet page, that list is, in itself, neutral and does not make it possible to ascertain the context surrounding the original publication.  
34      Accordingly, the question arises whether, when conducting the weighing-up exercise under Article 12(b) and point (a) of the first paragraph of Article 14 of Directive 95/46 or Article 17(3)(a) of the GDPR, account must be taken solely of the thumbnail as such in the neutral context of the list of results or whether account must also be taken of the original context of the publication of the corresponding image.  
35      In that regard, the referring court notes that, in the case in the main proceedings, which concerns persons who are not known to the general public, the photographs in question do not, in themselves, contribute to public debate and do not satisfy a compelling need for information in accordance with the provisions referred to in the preceding paragraph. However, in connection with the 4 June 2015 article published on the g-net website, the photographs play an important role in substantiating the message contained in that article, which is that the applicants in the main proceedings, by virtue of their position as founders and managers of the fourth company and of the group of companies referred to in paragraph 15 of the present judgment, enjoy a high standard of living and possess luxury goods, whilst the employees, distributors and customers of those companies are uncertain as to the safety of the investments made. Consequently, if account ought to be taken of the context in which those photographs were initially published, their publication as thumbnails in the list of results would have to be regarded as justified, provided that the text accompanying them is itself lawful.  
36      According to the referring court, one factor militating in favour of taking account of the context of the original publication lies in the fact that, technically, thumbnails constitute links referring to the third party’s internet page. Similarly, it is well known that the informed average user of an image search engine is aware of the fact that the thumbnails brought together by the search engine in a list of results are taken from third party publications and that the photographs corresponding to those thumbnails are displayed, in those publications, in a particular context.  
37      However, account should be taken of the fact that the original context of the publication of the images is neither stated nor otherwise visible when the thumbnail is displayed, unlike in the case of other referenced results. A user who, from the outset, is interested only in displaying the image has, as a general rule, no reason to seek out the source and the original context of the publication.  
38      According to the referring court, it therefore appears logical, for the purposes of assessing the lawfulness of the data processing by the search engine data controller concerned, to include in the weighing-up exercise referred to in point (a) of the first paragraph of Article 14 of Directive 95/46 or Article 17(3) of the GDPR only the rights and interests which are apparent from the thumbnail itself.  
39      In those circumstances, the Bundesgerichtshof (Federal Court of Justice) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is it compatible with the data subject’s right to respect for private life (Article 7 of the [Charter]) and to protection of personal data (Article 8 of the Charter) if, within the context of the weighing-up of conflicting rights and interests arising from Articles 7, 8, 11 and 16 of the Charter, within the scope of the examination of his [or her] request for de-referencing brought against the data controller of an internet search engine, pursuant to Article 17(3)(a) of [the GDPR], when the link, the de-referencing of which [that person] is requesting, leads to content that includes factual claims and value judgments based on factual claims the truth of which is denied by the data subject, and the lawfulness of which depends on the question of the extent to which the factual claims contained in that content are true, the national court also concentrates conclusively on the issue of whether the data subject could reasonably seek legal protection against the content provider, for instance by means of interim relief, and thus at least provisional clarification on the question of the truth of the content displayed by the search engine data controller could be provided?  
(2)      In the case of a request for de-referencing made against the data controller of an internet search engine, which in a name search searches for photos of natural persons which third parties have introduced into the internet in connection with the person’s name, and which displays the photos which it has found in its search results as preview images (thumbnails), within the context of the weighing-up of the conflicting rights and interests arising from Articles 7, 8, 11 and 16 of the Charter pursuant to Article 12(b) and [point (a) of the first paragraph of Article 14] of Directive [95/46 or] Article 17(3)(a) of [the GDPR], should the context of the original third-party publication be conclusively taken into account, even if the third-party website is linked by the search engine when the preview image is displayed but is not specifically named, and the resulting context is not shown with it by the internet search engine?’  
   
Consideration of the questions referred  
   
The first question  
   
Admissibility  
40      Google expresses doubts as to whether the first question is admissible, on the ground that the problem which it raises is hypothetical in nature. In particular, the solution suggested by the referring court takes the form of an abstract construction which is unrelated to the facts at issue in the case in the main proceedings. In its view, the Court also does not have the necessary material to provide a useful answer to that question.  
41      In that regard, it should be noted that, according to settled case-law, in the context of the cooperation between the Court and the national courts provided for in Article 267 TFEU, it is solely for the national court before which a dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions submitted by the national court concern the interpretation of EU law, the Court of Justice is, in principle, bound to give a ruling (judgment of 15 July 2021,   
The Department for Communities in Northern Ireland  
, C-709/20, EU:C:2021:602, paragraph 54 and the case-law cited).  
42      The Court may refuse to rule on a question referred by a national court for a preliminary ruling only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 15 July 2021,   
The Department for Communities in Northern Ireland  
, C-709/20, EU:C:2021:602, paragraph 55 and the case-law cited).  
43      In the present case, as the Advocate General observed in point 22 of his Opinion, the referring court has provided a sufficiently precise and comprehensive picture of the factual and legal context underlying the dispute in the main proceedings and has sufficiently substantiated the need, in that context, to obtain an answer to the question submitted.  
44      In that connection, it should be pointed out that the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 35). Where the data subject brings an action against the operator of the search engine, the rights, interests and restrictions involved are not, therefore, necessarily the same as in the context of an action brought against a content provider, with the result that a specific weighing-up exercise for the purposes of examining a request for de-referencing under Article 17 of the GDPR is necessary.  
45      It is apparent from the considerations set out by the referring court that the Court’s answer to the question concerning, first, the extent of the obligations and responsibilities incumbent on the operator of a search engine in processing a request for de-referencing based on the alleged inaccuracy of the information in the referenced content and, second, the burden of proof imposed on the data subject as regards that inaccuracy is capable of having a direct impact on the assessment, by the referring court, of the action in the main proceedings, regardless of whether the applicants in the main proceedings are in a position to obtain effective judicial protection as against the content provider concerning publication on the internet of the allegedly inaccurate content.  
46      As the Advocate General observed in point 22 of his Opinion, the fact that the referring court’s questions regarding the methodology which it considers to be applicable in a situation such as that at issue in the main proceedings are expressed in general and abstract terms does not mean that the question referred to the Court in that regard is hypothetical.  
47      It follows that the first question is admissible.  
   
Substance  
48      By its first question, the referring court asks, in essence, whether Article 17(3)(a) of the GDPR must be interpreted as meaning that, within the context of the weighing-up exercise which is to be undertaken between the rights referred to in Articles 7 and 8 of the Charter, on the one hand, and those referred to in Articles 11 and 16 of the Charter, on the other hand, for the purposes of examining a request for de-referencing made to the operator of a search engine seeking the removal of a link to content containing claims which the person who submitted the request regards as inaccurate from the list of search results, that de-referencing is subject to the condition that the question of the accuracy of the referenced content has been resolved, at least provisionally, in an action brought by that person against the provider of that content, where there is a reasonable possibility of obtaining such judicial protection.  
49      As a preliminary point, it must be recalled, first, that the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of Article 2(b) of Directive 95/46 and points 1 and 2 of Article 4 of the GDPR when that information contains personal data and, second, that the operator of the search engine must be regarded as the ‘controller’ in respect of that processing within the meaning of Article 2(d) of that directive and Article 4(7) of that regulation (see, to that effect, judgments of 13 May 2014,  
 Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 41, and of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 35).  
50      Indeed, as recalled in paragraph 44 of the present judgment, the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page. In addition, that activity plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject’s name, including to internet users who otherwise would not have found the internet page on which those data are published. Also, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users’ access to that information may, when users carry out their search on the basis of an individual’s name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject (see, to that effect, judgments of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraphs 36 and 37, and of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 36).  
51      Therefore, inasmuch as the activity of a search engine is liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 and of the GDPR in order that the guarantees laid down by that directive and that regulation may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved (see, to that effect, judgments of 13 May 2014,  
 Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 38, and of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 37).  
52      As regards the extent of the responsibility and specific obligations of the operator of a search engine, the Court has already stated that that operator is responsible not because personal data appear on an internet page published by a third party, but because of the referencing of that page and, in particular, the display of the link to that internet page in the list of results presented to internet users following a search carried out on the basis of an individual’s name, since such a display of the link in such a list is liable significantly to affect the data subject’s fundamental rights to privacy and to the protection of the personal data relating to him or her (see, to that effect, judgments of 13 May 2014,  
 Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 80, and of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 46).  
53      In those circumstances, having regard to the responsibilities, powers and capabilities of the operator of a search engine as the controller of the processing carried out in connection with the activity of the search engine, the prohibitions and restrictions laid down by Directive 95/46 and by the GDPR can apply to that operator only by reason of that referencing and thus via a verification, under the supervision of the competent national authorities, on the basis of a request by the data subject (see, to that effect, judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
 (C-136/17, EU:C:2019:773, paragraph 47).  
54      As regards such a request, the GDPR contains, in Article 17, a provision which specifically governs the ‘right to erasure’, also known as the ‘right to be forgotten’. Although paragraph 1 of that article provides that the data subject has, in principle, for the reasons listed therein, the right to obtain the erasure of personal data relating to him or her by the controller, it states, in paragraph 3, that that right may not be relied on where the processing in question is necessary on account of one of the grounds listed, which include, in Article 17(3)(a), exercising the right relating, in particular, to freedom of information.  
55      Accordingly, the operator of a search engine who receives a request for de-referencing must ascertain whether the inclusion of the link to the internet page in question in the list displayed following a search carried out on the basis of the data subject’s name is necessary for exercising the right to freedom of information of internet users potentially interested in accessing that internet page by means of a search, a right protected by Article 11 of the Charter (see, by analogy, judgment of 24 September 2019,  
 GC and Others (De-referencing of sensitive data)  
 (C-136/17, EU:C:2019:773, paragraph 66).  
56      The fact that Article 17(3)(a) of the GDPR expressly provides that the data subject’s right to erasure is excluded where processing is necessary for the exercise of the right of information, guaranteed in Article 11 of the Charter, is an expression of the fact that the right to protection of personal data is not an absolute right but, as recital 4 of the regulation states, must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality (see, to that effect, judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data),   
 C-136/17, EU:C:2019:773, paragraph 57 and the case-law cited).  
57      In that context, it should be recalled that Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 58 and the case-law cited).  
58      The GDPR, and in particular Article 17(3)(a), thus expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter, on the one hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other (judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 59).  
59      It should be added that Article 7 of the Charter, regarding the right to respect for private and family life, contains rights corresponding to those guaranteed in Article 8(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (‘the ECHR’), and that the protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR (ECtHR, 27 June 2017,  
 Satakunnan Markkinapörssi oy and satamedia oy v. Finland  
, CE:ECHR:2017:0627JUD000093113, § 137). In accordance with Article 52(3) of the Charter, Article 7 of the Charter is thus to be given the same meaning and the same scope as Article 8(1) ECHR, as interpreted by the case-law of the European Court of Human Rights. The same is true of Article 11 of the Charter and Article 10 ECHR (see to that effect, judgment of 14 February 2019,   
Buivids  
, (C-345/17, EU:C:2019:122, paragraph 65 and the case-law cited).  
60      It is apparent from the case-law of the European Court of Human Rights that, as regards the publication of data, for the purposes of striking a balance between the right to respect for private life and the right of freedom of expression and information, a number of relevant criteria must be taken into consideration, such as contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, the form and consequences of the publication, the manner and circumstances in which the information was obtained as well and its veracity (see, to that effect, ECtHR, 27 June 2017,  
 Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland  
, CE:ECHR:2017:0627JUD000093113, § 165).  
61      It is in the light of those considerations that an examination must be made of the conditions in which the operator of a search engine is required to accede to a request for de-referencing and thus to remove from the list of results displayed following a search on the basis of the data subject’s name, the link to an internet page on which that personal data specific to that person appear, on the ground that the referenced content contains claims which that person regards as inaccurate (see, to that effect, judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
 (C-136/17, EU:C:2019:773, paragraph 60).  
62      In that regard, it should be noted, first of all, that, while the data subject’s rights protected by Articles 7 and 8 of the Charter override, as a general rule, the legitimate interest of internet users who may be interested in accessing the information in question, that balance may, however, depend on the relevant circumstances of each case, in particular on the nature of that information and its sensitivity for the data subject’s private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life (judgments of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 81, and of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 66).  
63      In particular, where the data subject plays a role in public life, that person must display a greater degree of tolerance, since he or she is inevitably and knowingly exposed to public scrutiny (see, to that effect, ECtHR, 6 October 2022,   
Khural and Zeynalov v. Azerbaijan  
, CE:ECHR:2022:1006JUD005506911, § 41 and the case-law cited).  
64      The question of whether or not the referenced content is accurate also constitutes a relevant factor when assessing the conditions for application laid down in Article 17(3)(a) of the GDPR, for the purpose of assessing whether the right of internet users to information and the content provider’s freedom of expression may override the rights of the person requesting de-referencing.  
65      In that regard, and as stated, in essence, by the Advocate General in point 30 of his Opinion, while, in certain circumstances, the right to freedom of expression and information may override the rights to private life and to protection of personal data, in particular where the data subject plays a role in public life, that relationship is in any event reversed where, at the very least, a part – which is not minor in relation to the content as a whole – of the information referred to in the request for de-referencing proves to be inaccurate. In such a situation, the right to inform and the right to be informed cannot be taken into account, since they cannot include the right to disseminate and have access to such information.  
66      It should be added that, while the issue of whether or not the assertions in the referenced content are accurate is relevant for the application of Article 17(3)(a) of the GDPR, a distinction must be drawn between factual assertions and value judgements. While the existence of facts can be demonstrated, the truth of value judgments is not susceptible of proof (see, to that effect, ECtHR, 23 April 2015,   
Morice v. France  
, CE:ECHR:2015:0423JUD002936910, § 126).  
67      Next, it is necessary to determine, first, whether, and if so to what extent, it is for the person who has submitted the request for de-referencing to provide evidence to support his or her claim relating to the inaccuracy of the information in the referenced content and, second, whether the operator of the search engine must seek to clarify the facts itself in order to establish whether the allegedly inaccurate information is or is not accurate.  
68      As regards, in the first place, the obligations of the person requesting de-referencing on account of the referenced content being inaccurate, it is for that person to establish the manifest inaccuracy of the information found in that content or, at the very least, of a part – which is not minor in relation to the content as a whole – of that information. However, in order to avoid imposing on that person an excessive burden which is liable to undermine the practical effect of the right to de-referencing, that person has to provide only evidence that, in the light of the circumstances of the particular case, can reasonably be required of him or her to try to find in order to establish that manifest inaccuracy. In that regard, that person cannot be required, in principle, to produce, as from the pre-litigation stage, in support of his or her request for de-referencing made to the operator of the search engine, a judicial decision made against the publisher of the website in question, even in the form of a decision given in interim proceedings. To impose such an obligation on that person would have the effect of imposing an unreasonable burden on him or her.  
69      As regards, in the second place, the obligations and responsibilities incumbent on the operator of the search engine, it is true that the operator of the search engine must, in order to determine whether content may continue to be included in the list of search results carried out using its search engine following a request for de-referencing, take into account all the rights and interests involved and all the circumstances of the case.  
70      However, when assessing the conditions for application laid down in Article 17(3)(a) of the GDPR, that operator cannot be required to play an active role in trying to find facts which are not substantiated by the request for de-referencing, for the purposes of determining whether that request is well founded.  
71      Accordingly, when such a request is processed, the operator of the search engine concerned cannot be required to investigate the facts and, to that end, to organise an adversarial debate with the content provider seeking to obtain missing information concerning the accuracy of the referenced content. In so far as it would require the operator of the search engine to contribute to establishing itself whether or not the referenced content is accurate, such an obligation would impose on that operator a burden in excess of what can reasonably be expected of it in the light of its responsibilities, powers and capabilities, within the meaning of the case-law referred to in paragraph 53 of the present judgment. That obligation would thereby entail a serious risk that content meeting the public’s legitimate and compelling need for information would be de-referenced and would thereby become difficult to find on the internet. In that regard, there would be a real risk of a deterrent effect on the exercise of freedom of expression and of information if the operator of the search engine undertook such a de-referencing exercise quasi-systematically, in order to avoid having to bear the burden of investigating the relevant facts for the purpose of establishing whether or not the referenced content was accurate.  
72      Accordingly, where the person who has made a request for de-referencing submits relevant and sufficient evidence capable of substantiating his or her request and of establishing the manifest inaccuracy of the information found in the referenced content or, at the very least, of a part – which is not minor in relation to the content as a whole – of that information, the operator of the search engine is required to accede to that request for de-referencing. The same applies where the data subject submits a judicial decision made against the publisher of the website, which is based on the finding that information found in the referenced content – which is not minor in relation to that content as a whole – is, at least prima facie, inaccurate.  
73      By contrast, where the inaccuracy of such information found in the referenced content is not obvious, in the light of the evidence provided by the data subject, the operator of the search engine is not required, where there is no such judicial decision, to accede to such a request for de-referencing. Where the information in question is likely to contribute to a debate of public interest, it is appropriate, in the light of all the circumstances of the case, to place particular importance on the right to freedom of expression and of information.  
74      It should be added that, in accordance with what has been stated in paragraph 65 of the present judgment, it would also be disproportionate to de-reference articles, with the result that accessing all of them on the internet would be difficult, in a situation where only certain information of minor importance, in relation to the content found in those articles as a whole, proves to be inaccurate.  
75      Lastly, it must be stated that, where the operator of a search engine does not grant the request for de-referencing, the data subject must be able to bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders that controller to adopt the necessary measures (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
 (C-131/12, EU:C:2014:317, paragraph 77). It is, in particular, for the judicial authorities to ensure a balance is struck between competing interests, since they are best placed to carry out a complex and detailed balancing exercise, which takes account of all the criteria and all the factors established by the relevant case-law of the Court of Justice and of the European Court of Human Rights.  
76      However, where administrative or judicial proceedings concerning the alleged inaccuracy of information found in referenced content are initiated and where the existence of those proceedings has been brought to the attention of the operator of the search engine concerned, it is for that operator, for the purposes, inter alia, of providing internet users with information which continues to be relevant and up-to-date, to add to the search results a warning concerning the existence of such proceedings.  
77      In the light of all the foregoing, the answer to the first question is that Article 17(3)(a) of the GDPR must be interpreted as meaning that, within the context of the weighing-up exercise which is to be undertaken between the rights referred to in Articles 7 and 8 of the Charter, on the one hand, and those referred to in Article 11 of the Charter, on the other hand, for the purposes of examining a request for de-referencing made to the operator of a search engine seeking the removal of a link to content containing claims which the person who submitted the request regards as inaccurate from the list of search results, that de-referencing is not subject to the condition that the question of the accuracy of the referenced content has been resolved, at least provisionally, in an action brought by that person against the content provider.  
   
The second question  
   
The applicable law ratione temporis  
78      By its second question, the referring court requests an interpretation of Article 12(b) and point (a) of the first paragraph of Article 14 of Directive 95/46 as well as of Article 17(3)(a) of the GDPR. It states, in that regard, that, while the request to have Google de-reference, on a long-term basis, the links to the articles at issue in the main proceedings falls ratione temporis within the scope of the GDPR, the request that Google put an end to the display, in the form of thumbnails, of photographs of the applicants in the main proceedings contained in the 4 June 2015 article falls ratione temporis within the scope of Directive 95/46, given that those photographs, unlike the links, were no longer displayed by the search engine operated by Google on the date when the GDPR entered into force.  
79      In that regard, there is no need to distinguish between the provisions of Directive 95/46 and those of the GDPR referred to in the second question referred for a preliminary ruling, since the scope of all of those provisions must be regarded as similar for the purposes of the interpretation which the Court is required to give in the present case (see, by analogy, judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 58 and the case-law cited).  
80      Consequently, in order to provide useful answers to the second question, it must be examined from the perspective of both Directive 95/46 and the GDPR.  
   
Admissibility  
81      Google also expresses doubts as to whether the second question is admissible, on the ground that the problem which it raises is hypothetical. First of all, Google takes the view that the subject matter of the dispute in the main proceedings is not a request to de-reference the results of an image search carried out on the basis of the names of the applicants in the main proceedings, but rather a general prohibition on displaying thumbnails corresponding to photographs illustrating one of the three articles at issue in the main proceedings. Next, Google argues that the thumbnails have not been available on the g-net website since September 2017 and the articles since 28 June 2018. Lastly, Google states that it introduced a new version of its image search engine as from 2018, in which the abbreviated title of the internet page specifically referenced and the internet address or a part of it are displayed on the results page under each thumbnail in the form of an additional link.  
82      Pursuant to the principles identified by the case-law of the Court referred to in paragraphs 41 and 42 of the present judgment, it must be stated, first of all, that, in the present case, it is not obvious from the file before the Court that the interpretation of the provisions of Directive 95/46 and the GDPR, as sought by the referring court in the context of the assessment of the substance of the request seeking to have the display of the photographs brought to an end, bears no relation to the actual facts of the main action or its purpose.  
83      As regards, in particular, the fact that the photographs and articles at issue in the main proceedings no longer appear on the g-net website, it is important to note, as the referring court has observed, that the removal of that content appears to be merely temporary, as shown by the statement on the g-net website that it is ‘currently’ impossible to access those articles. In those circumstances, it cannot be ruled out that those articles may be re-posted online in the future and may once again be referenced by Google’s search engine. That is all the more so since Google continues to take the view that the request for de-referencing at issue in the main proceedings is unjustified and since Google continues to refuse to accede to that request.  
84      Moreover, the interest in a response from the Court concerning the interpretation of the relevant provisions of Directive 95/46 and of the GDPR, in the context of the request seeking to have brought to an end the display, in the form of thumbnails, of the photographs at issue in the case in the main proceedings, cannot be called into question either by the fact, relied on by Google, that the applicants in the main proceedings have not limited their request to searches on the basis of their names, or by the fact that Google has introduced a new version of its image search engine in which the abbreviated title of the internet page specifically referenced and the internet address or a part of it are displayed on the results page under each thumbnail in the form of an additional link.  
85      First, even if the request of the applicants in the main proceedings to bring to an end the display, in the form of thumbnails, of the photographs representing them were not limited to searches carried out on the basis of their names, the fact remains that that request covers a display resulting from such searches. In those circumstances, it cannot be held that the interpretation sought by virtue of the second question clearly bears no relation to the actual facts of the main action or its purpose.  
86      Second, as regards the introduction in the image search of an additional link showing the internet page on which they were originally published, in accordance with the settled case-law of the Court, it is for the national courts to establish the facts on the basis of which the dispute in the main proceedings must be resolved and to decide the extent to which subsequent developments in the search engine concerned are relevant in that regard.  
87      It follows that the second question is admissible.  
   
Substance  
88      By its second question, the referring court asks, in essence, whether Article 12(b) and point (a) of the first paragraph of Article 14 of Directive 95/46 as well as Article 17(3)(a) of the GDPR must be interpreted as meaning that, in the context of the weighing-up exercise which is to be undertaken between the rights referred to in Articles 7 and 8 of the Charter, on the one hand, and those referred to in Articles 11 and 16 of the Charter, on the other hand, for the purposes of examining a request for de-referencing made to the operator of a search engine seeking the removal from the results of an image search carried out on the basis of the name of a natural person of photographs displayed in the form of thumbnails representing that person, the original context of the publication of those photographs on the internet must be conclusively taken into account.  
89      That question thereby referred to the Court involves a request which seeks the removal of the photographs displayed in the form of thumbnails, which illustrated the article published on the g-net website on 4 June 2015, from the results of the image search carried out on the basis of the names of the applicants in the main proceedings. In that regard, the referring court seeks, in particular, to ascertain whether, for the purposes of assessing whether that request is well founded, account should be taken solely of the informative value of the thumbnails as such, in the neutral context of the list of results, or whether regard must also be had to the original context of the publication of the photographs, which is not apparent solely from the display of thumbnails in the context of the list of results.  
90      As a preliminary point, it should be noted, as the Advocate General did in point 53 of his Opinion, that image searches carried out by means of an internet search engine on the basis of a person’s name are subject to the same principles as those which apply to internet page searches and the information contained in them. The Court’s case-law referred to in paragraphs 49 to 61 of the present judgment therefore also applies to the processing of a request for de-referencing which seeks the removal of photographs displayed in the form of thumbnails from the results of an image search.  
91      In that regard, it is important to state, first of all, that the display, in the results of an image search, of photographs of natural persons in the form of thumbnails constitutes processing of personal data in respect of which the operator of the search engine concerned, as ‘controller’ within the meaning of Article 2(d) of Directive 95/46 and Article 4(7) of the GDPR, must, within the framework of its responsibilities, powers and capabilities, ensure compliance with the requirements contained in those provisions.   
92      Next, it should be noted that the question referred concerns the specific method of searching for images offered by certain search engines, such as the search engine at issue in the main proceedings, by means of which internet users can search for information of any kind which takes the form of graphic content (photographs, representations of paintings, designs, graphs, tables, and so forth). When conducting such a search, the search engine generates a list of results consisting of thumbnails providing a link to internet pages containing both the search terms used and the graphic content set out in that list.  
93      In that regard, it has been held that, since the inclusion in the list of results, displayed following a search made on the basis of a person’s name, of an internet page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of that person and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject’s fundamental right to privacy than the publication on the internet page (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 87).  
94      That is all the more so where, following a search by name, photographs of the data subject are displayed in the form of thumbnails, that display being such as to constitute a particularly significant interference with the data subject’s rights to private life and that person’s personal data referred to in Articles 7 and 8 of the Charter.  
95      A person’s image constitutes one of the chief attributes of his or her personality as it reveals the person’s unique characteristics and distinguishes the person from others. The right to the protection of one’s image is thus one of the essential components of personal development and mainly presupposes that person’s control over the use of that image, including the right to refuse publication of it. It follows that, while freedom of expression and of information undoubtedly includes the publication of photographs, the protection of the right to privacy takes on particular importance in that context since photographs are capable of conveying particularly personal or even intimate information about an individual or his or her family (see, to that effect, ECtHR, 7 February 2012,   
Von Hannover v. Germany  
, CE:ECHR:2012:0207JUD004066008, §§ 95, 96 and 103 and the case-law cited).  
96      Consequently, when the operator of a search engine receives a request for de-referencing which seeks the removal, from the results of an image search carried out on the basis of the name of a person, of photographs displayed in the form of thumbnails representing that person, it must ascertain whether displaying the photographs in question is necessary for exercising the right to freedom of information of internet users who are potentially interested in accessing those photographs by means of such a search, a right protected by Article 11 of the Charter (see, by analogy, judgment of 24 September 2019,  
 GC and Others (De-referencing of sensitive data)  
 (C-136/17, EU:C:2019:773, paragraph 66).  
97      In that regard, the contribution to a debate of public interest is an essential factor to be taken into consideration when striking a balance between competing fundamental rights, for the purposes of assessing whether what prevails are (i) the data subject’s rights to respect for private life and to protection of his or her personal data or (ii) the rights to freedom of expression and information.  
98      In so far as the search engine displays photographs of the data subject outside the context in which they are published on the referenced internet page, most often in order to illustrate the text elements contained in that page, it is necessary to establish whether that context must nevertheless be taken into consideration when striking a balance between the competing rights and interests.  
99      In that context, as the Advocate General observed in point 54 of his Opinion, the question whether that assessment must also include the content of the internet page containing the photograph displayed in the form of a thumbnail, the removal of which is sought, depends on the purpose and nature of the processing at issue.  
100    As regards, in the first place, the purpose of the processing at issue, it should be noted that the publication of photographs as a non-verbal means of communication is likely to have a stronger impact on internet users than text publications. Photographs are, as such, an important means of attracting internet users’ attention and may encourage an interest in accessing the articles they illustrate. Since, in particular, photographs are often open to a number of interpretations, displaying them in the list of search results as thumbnails may, in accordance with what has been stated in paragraph 95 of the present judgment, result in a particularly serious interference with the data subject’s right to protection of his or her image, which must be taken into account when weighing-up competing rights and interests.  
101    Consequently, a separate weighing-up of competing rights and interests is required depending on whether the case concerns, on the one hand, articles containing photographs which are published on an internet page and which, when placed into their original context, illustrate the information provided in those articles and the opinions expressed in them, or, on the other hand, photographs displayed in the list of results in the form of thumbnails by the operator of a search engine outside the context in which they were published on the original internet page.  
102    In that regard, it must be recalled that not only does the ground justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing-up of the rights and interests at issue may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of that internet page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his or her private life, are not necessarily the same (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 86).  
103    As regards, in the second place, the nature of the processing carried out by the operator of the search engine, it must be observed, as did the Advocate General in point 55 of his Opinion, that, by retrieving the photographs of natural persons published on the internet and displaying them separately, in the results of an image search, in the form of thumbnails, the operator of a search engine offers a service in which it carries out autonomous processing of personal data which is distinct both from that of the publisher of the internet page from which the photographs are taken and from that, for which the operator is also responsible, of referencing that page.  
104    Therefore, an autonomous assessment of the activity of the operator of the search engine, which consists of displaying results of an image search, in the form of thumbnails, is necessary, given that the additional interference with fundamental rights resulting from such activity may be particularly intense owing to the aggregation, in a search by name, of all information concerning the data subject which is found on the internet. In the context of that autonomous assessment, account must be taken of the fact that the display of the photographs in the form of thumbnails on the internet constitutes, in itself, the result sought by the internet user, regardless of his or her subsequent decision to access the original internet page or not.  
105    It should be added that such a specific weighing-up exercise, which takes account of the autonomous nature of the data processing performed by the operator of the search engine, is without prejudice to the possible relevance of text elements which may directly accompany the display of a photograph in the list of search results, since such elements are capable of casting light on the informative value of that photograph for the public and, consequently, of influencing the weighing-up of the rights and interests involved.  
106    In the present case, it is apparent from the observations in the order for reference that, while the photographs of the applicants in the main proceedings contribute, in the context of the 4 June 2015 article of which they form part, to conveying the information and opinions expressed therein, those photographs, outside that context, when they appear solely in the form of thumbnails in the list of results displayed following a search carried out by the search engine, have little informative value. It follows that, if the request for de-referencing of that article were to be rejected, on the ground that freedom of expression and of information must prevail over the rights of the applicants in the main proceedings to respect for their private life and to protection of their personal data, that fact would be without prejudice to the appropriate outcome of the request for removal of those photographs displayed in the form of thumbnails in the list of results.  
107    By contrast, if the request for de-referencing of the 4 June 2015 article at issue were to be granted, the display, in the form of thumbnails, of the photographs contained in that article would have to be removed. If that display were retained, the practical effect of de-referencing the article would be compromised since internet users would continue to have access to the entire article, by virtue of the link contained in the thumbnails which leads to the internet page on which the article from which the thumbnails are taken is published.  
108    In the light of all the foregoing, the answer to the second question is that Article 12(b) and point (a) of the first paragraph of Article 14 of Directive 95/46 as well as Article 17(3)(a) of the GDPR must be interpreted as meaning that, in the context of the weighing-up exercise which is to be undertaken between the rights referred to in Articles 7 and 8 of the Charter, on the one hand, and those referred to in Article 11 of the Charter, on the other hand, for the purposes of examining a request for de-referencing made to the operator of a search engine seeking the removal from the results of an image search carried out on the basis of the name of a natural person of photographs displayed in the form of thumbnails representing that person, account must be taken of the informative value of those photographs regardless of the context of their publication on the internet page from which they are taken, but taking into consideration any text element which accompanies directly the display of those photographs in the search results and which is capable of casting light on the informative value of those photographs.  
   
Costs  
109    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 17(3)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),  
must be interpreted as meaning that within the context of the weighing-up exercise which is to be undertaken between the rights referred to in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, on the one hand, and those referred to in Article 11 of the Charter of Fundamental Rights, on the other hand, for the purposes of examining a request for de-referencing made to the operator of a search engine seeking the removal of a link to content containing claims which the person who submitted the request regards as inaccurate from the list of search results, that de-referencing is not subject to the condition that the question of the accuracy of the referenced content has been resolved, at least provisionally, in an action brought by that person against the content provider.   
2.        
Article 12(b) and point (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as Article 17(3)(a) of Regulation 2016/679  
must be interpreted as meaning that in the context of the weighing-up exercise which is to be undertaken between the rights referred to in Articles 7 and 8 of the Charter of Fundamental Rights, on the one hand, and those referred to in Article 11 of the Charter of Fundamental Rights, on the other hand, for the purposes of examining a request for de-referencing made to the operator of a search engine seeking the removal from the results of an image search carried out on the basis of the name of a natural person of photographs displayed in the form of thumbnails representing that person, account must be taken of the informative value of those photographs regardless of the context of their publication on the internet page from which they are taken, but taking into consideration any text element which accompanies directly the display of those photographs in the search results and which is capable of casting light on the informative value of those photographs.

ID: 7024c6a8-dc90-4dae-855f-369f8be1d62b

of 16 Feb 2023, C-349/21 (  
HYA and Others (Motivation des autorisations des écoutes téléphoniques)  
)  
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
   
JUDGMENT OF THE COURT (Third Chamber)  
16 February 2023 (\*)  
(Reference for a preliminary ruling – Telecommunications sector – Processing of personal data and the protection of privacy – Directive 2002/58/EC – Article 15(1) – Restriction of the confidentiality of electronic communications – Judicial decision authorising the interception, recording and storage of telephone conversations of persons suspected of having committed a serious intentional offence – Practice whereby the decision is drawn up in accordance with a pre-drafted template text that does not contain individualised reasons – Second paragraph of Article 47 of the Charter of Fundamental Rights of the European Union – Obligation to state reasons)  
In Case C-349/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Spetsializiran nakazatelen sad (Specialised Criminal Court, Bulgaria), made by decision of 3 June 2021, received at the Court on 4 June 2021, in the proceedings  
HYA,  
IP,  
DD,  
ZI,  
SS,  
the other party to the proceedings being:  
Spetsializirana prokuratura  
THE COURT (Third Chamber),  
composed of K. Jürimäe, President of the Chamber, M. Safjan (Rapporteur), N. Piçarra, N. Jääskinen and M. Gavalec, Judges,  
Advocate General: A.M. Collins,  
Registrar: R. Stefanova-Kamisheva, Administrator,  
having regard to the written procedure and further to the hearing on 6 July 2022,  
after considering the observations submitted on behalf of:  
IP, by H. Georgiev, advokat,  
DD, by V. Vasilev, advokat,  
the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
Ireland, by M. Browne and D. Fennelly, Barrister-at-Law, and by A. Joyce and M. Lane, acting as Agents,  
the European Commission, by C. Georgieva and H. Kranenborg, P.-J. Loewenthal and F. Wilman, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 13 October 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).  
2        The request has been made in criminal proceedings brought against HYA, IP, DD, ZI and SS for participation in an organised criminal gang.  
   
Legal context  
   
European Union law  
   
Directive 2002/58  
3        Recital 11 of Directive 2002/58 states:  
‘Like Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950 (‘the ECHR’)], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the [ECHR].’  
4        The first paragraph of Article 2 of that directive provides:  
‘Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.’  
5        Article 5(1) of that directive provides:  
‘Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.’  
6        Article 15(1) of that directive is worded as follows:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].’  
   
Regulation (EU) 2016/679  
7        Under Article 4(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1):  
‘For the purposes of this Regulation:  
…  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…’  
8        Article 94(2) of that regulation provides:  
‘References to the repealed Directive [95/46] shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.’  
   
Bulgarian law  
9        Article 121(4) of the Bulgarian Constitution provides that ‘judicial acts shall state reasons’.  
10      Article 34 of the Nakazatelno protsesualen kodeks (Code of Criminal Procedure), in the version applicable to the dispute in the main proceedings (‘the NPK’), provides that ‘any act of the court shall contain … reasons …’.  
11      Article 172 of the NPK is worded as follows:  
‘(1)      The authorities responsible for the pre-trial stage of the proceedings may make use of special investigative methods … which shall serve to document the activities of the monitored persons …  
(2)      Special investigative methods shall be used where that is necessary for the investigation of serious intentional criminal offences under Chapter I, Chapter II, Sections I, II, IV, V, VIII and IX, Chapter III, Section III, Chapter V, Sections I to VII, Chapter VI, Sections II to IV, Chapter VIII, Chapter VIIIa, Chapter IXa, Chapter XI, Sections I to IV, Chapter XII, Chapter XIII and Chapter XIV, and for the criminal offences under Article 219(4), second situation, Article 220(2), Article 253, Article 308(2), (3) and (5), second sentence, Article 321, Article 321a, Article 356k and Article 393 of the Special Part of the Nakazatelen kodeks (Criminal Code), where the establishment of the circumstances in question is impossible in any other way, or is accompanied by exceptional difficulties.’  
12      Under Article 173 of the NPK:  
‘(1)      In order to make use of special investigative methods in the pre-trial stage of the proceedings, the supervising public prosecutor shall submit to the court a written request stating reasons. Prior to the submission of the application, the latter shall advise the administrative officer of the public prosecutor’s office concerned.  
(2)      The application must contain:  
1.      Information relating to the criminal offence for which the investigation requires the use of special investigative methods;  
2.      A description of the actions taken and their outcome;  
3.      Information relating to the persons or premises to which the special investigative methods apply;  
4.      The operating methods to be applied;  
5.      The duration of the use requested and the reasons for which that duration is requested;  
6.      The reasons for which the necessary data cannot be collected otherwise or can be collected only with extreme difficulty.’  
13      Article 174(3) and (4) of the NPK state:  
‘(3)      An authorisation for the use of special investigative methods in proceedings within the jurisdiction of the Spetsializiran nakazatelen sad [(Specialised Criminal Court, Bulgaria)] shall be granted in advance by its President …  
(4)      The authority referred to in paragraphs 1 to 3 shall rule by reasoned order …’  
14      Article 175 of the NPK is worded as follows:  
‘…  
(3)      The time period for applying special investigative methods shall not exceed:  
1.      twenty days in the case of Article 12(1)(4) of the zakon za spetsialnite razuznavatelni sredstva [(Law on special investigative methods)];  
2.      two months in the other cases.  
(4)      Where necessary, the time period referred to in paragraph 1 may be extended in accordance with Article 174:  
1.      by twenty days, but not exceeding sixty days in total in the cases referred to in paragraph 3(1);  
2.      but not exceeding six months in total in the cases referred to in paragraph 3(2)’.  
15      Article 3(1) of the zakon za spetsialnite razuznavatelni sredstva (Law on special investigative methods) of 8 October 1997 (DV No 95 of 21 October 1997, p. 2), in the version applicable to the dispute in the main proceedings (‘the ZSRS’), provides:  
‘Special investigative methods shall be used where that is necessary to prevent and detect serious intentional criminal offences under Chapter I, Chapter II, Sections I, II, IV, V, VIII and IX, Chapter III, Section III, Chapter V, Sections I to VII, Chapter VI, Sections II to IV, Chapter VIII, Chapter VIIIa, Chapter IXa, Chapter XI, Sections I to IV, Chapter XII, Chapter XIII and Chapter XIV, and for criminal offences under Article 219(4), second situation, Article 220(2), Article 253, Article 308(2), (3) and (5), second sentence, Article 321, Article 321a, Article 356k and Article 393 of the Special Part of the [Criminal Code], where the collection of the necessary information is impossible in any other way, or is accompanied by exceptional difficulties.’  
16      Article 6 of the ZSRS provides:  
‘In the event of listening, through the use of technical means, aurally or otherwise, the … telephone communications … of the monitored persons shall be intercepted.’  
17      Article 11 of the ZSRS is worded as follows:  
‘In the application of the modes of operation, evidence shall be provided by means of … audio recording … on a physical medium.’  
18      Article 12(1)(1) of the ZSRS provides:  
‘Special investigative methods shall be used for persons in respect of whom there is information and reasonable grounds to believe that they are preparing, committing or have committed any of the serious intentional criminal offences referred to in Article 3(1).’  
19      Article 13(1) of the ZSRS reads as follows:  
‘The following shall be entitled to request the use of special investigative methods and to make use of the information and material evidence gathered by means of those methods, in accordance with their powers:  
1.      the Directorate-General “National Police”, the Directorate-General “Combating Organised Crime”, the Directorate-General “Border Police”, the Directorate “Internal Security”, the regional directorates of the Ministry of the Interior, the specialised directorates (with the exception of the Directorate “Technical Operations”), the territorial directorates and the autonomous territorial divisions of the State agency “National Security”;  
2.      the “Military Intelligence” and “Military Police” services (under the Minister for Defence);  
3.      the State agency “Intelligence”.’  
20      Article 14(1)(7) of the ZSRS states:  
‘The use of special investigative methods shall require a reasoned written request from the relevant administrative head of the authorities referred to in Article 13(1) or the supervising public prosecutor, or, as the case may be, from the authority referred to in Article 13(3), and in the case of the directorate referred to in Article 13(1)(7), from its director. The application must state … the reasons why the collection of the necessary data is impossible in any other way, or a description of the extreme difficulties accompanying its collection.’  
21      Article 15(1) of the ZSRS provides:  
‘The heads of the authorities referred to in Article 13(1) or the supervising public prosecutor, and in the case of the directorate referred to in Article 13(1)(7), the President of the Commission for the combating of corruption and for the confiscation of illegally obtained assets, shall submit the application to the Presidents of the Sofiyski gradski sad (Sofia City Court, Bulgaria), the relevant regional or military courts, the Spetsializiran nakazatelen sad (Specialised Criminal Court), or to a Vice-President authorised by them, who shall, within 48 hours, authorise in writing the use of special investigative methods or refuse their use, stating the reasons for their decisions.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
22      Between 10 April and 15 May 2017, the Spetsializirana prokuratura (Specialised Public Prosecutor’s Office, Bulgaria) submitted seven applications to the President of the Spetsializiran nakazatelen sad (Specialised Criminal Court) for authorisation to use special investigative methods for the purpose of listening to and recording, as well as monitoring and tracing, the telephone conversations of IP, DD, ZI and SS, four persons suspected of having committed serious offences (‘the telephone tapping applications’).  
23      It is apparent from the order for reference that each of those telephone tapping applications gave a full, detailed and reasoned description of the subject matter of the application, the name and telephone number of the person concerned, the link between that number and that person, the evidence gathered up to that point and the role allegedly played by the person concerned in the criminal acts. Specific reasons were also given as to why the requested telephone tapping was necessary to gather evidence about the criminal activity under investigation and why and under what conditions it was impossible to gather this information by other means.  
24      The President of the Spetsializiran nakazatelen sad (Specialised Criminal Court) granted each of those applications on the same day that they were brought and, consequently, issued seven decisions authorising telephone tapping (‘the telephone tapping authorisations’).  
25      According to the Spetsializiran nakazatelen sad (Specialised Criminal Court), the referring court, the telephone tapping authorisations correspond to a pre-drafted template designed to cover all possible cases of authorisation, irrespective of the various circumstances of fact and law, other than the length of time during which the use of special investigative methods was authorised.  
26      In particular, those authorisations merely state that the statutory provisions to which they refer have been complied with, without identifying the authority which made the telephone tapping applications and without indicating the name and telephone number of each person concerned, the offence or offences referred to in Article 172(2) of the NPK and Article 3(1) of the ZSRS, the evidence leading to the suspicion of the commission of one or more of those offences or even the categories of persons and premises, referred to in Article 12 of the ZSRS, for which the use of special investigative methods has been authorised. Furthermore, the referring court states that those authorisations do not set out the arguments of the Specialised Public Prosecutor’s Office demonstrating, on the basis of Article 172 of the NPK and Article 14 of the ZSRS, that it is impossible to gather the information sought by any means other than telephone tapping, nor do they specify, with regard to Article 175 of the NPK, whether the period specified for the use of those methods is set for the first time or whether it is an extension of the time limit and on the basis of what assumptions and arguments that time limit has been decided.  
27      On foot of those authorisations, some of the conversations conducted by IP, DD, ZI and SS were recorded and stored in accordance with Article 11 of the ZSRS.  
28      On 19 June 2020, the Specialised Public Prosecutor’s Office accused those four persons, together with a fifth, HYA, of participating in an organised criminal gang for the purpose of enrichment, smuggling third-country nationals across Bulgarian borders, assisting them to enter Bulgarian territory illegally and receiving or giving bribes in connection with those activities. The accused include three agents of the Sofia airport border police.  
29      The referring court, hearing the merits of the case, states that the content of the recorded conversations is of direct relevance in determining whether the charges brought against IP, DD, ZI and SS are well founded.  
30      It explains that it is required, in advance, to review the validity of the procedure which led to the telephone tapping authorisations. In that context, it might be considered that the fact that those authorisations were drawn up in accordance with a pre-drafted template text that does not contain individualised reasons does not enable it to ascertain the reasons specifically relied on by the judge who granted those authorisations. Conversely, it would also be possible to take the view that, by acceding to the request of the Specialised Public Prosecutor’s Office, the judge who granted the telephone tapping authorisations accepted the reasons for those applications in full and endorsed them.  
31      While not doubting that the national legislation on telephone tapping, as it results in particular from the provisions of the NPK and the ZSRS, is compatible with Article 15(1) of Directive 2002/58, the referring court is uncertain whether a national practice such as that at issue in the main proceedings, according to which the obligation to state the reasons for the judicial decision authorising the use of special investigative methods following a reasoned request by the criminal authorities is satisfied where that decision, drawn up in accordance with a pre-drafted template which does not contain individualised reasons, merely states that the requirements laid down by that legislation, to which it refers, have been complied with, is compatible with the last sentence of Article 15(1) of that directive, read in the light of recital 11 thereof.  
32      In particular, that court points out that judicial decisions such as telephone tapping authorisations limit, with regard to the natural persons concerned, the rights and freedoms guaranteed in Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union (‘the Charter’). It also has doubts as to whether such a practice complies with the right to effective judicial protection, enshrined in Article 47 of the Charter, and the principle of proportionality as a general principle of EU law.  
33      If the answer is in the negative, the referring court asks whether EU law precludes an interpretation of national legislation such that recordings of telephone conversations authorised by a judicial decision which does not contain a statement of reasons may nevertheless be used as evidence in criminal proceedings.  
34      In those circumstances, the Spetsializiran nakazatelen sad (Specialised Criminal Court) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
(1)      Is a practice of national courts in criminal proceedings whereby the court authorises the interception, recording and storage of telephone conversations of suspects by means of a pre-drafted, generic text template in which it is merely asserted, without any individualisation, that the statutory provisions have been complied with compatible with Article 15(1) of Directive 2002/58 … read in conjunction with Article 5(1) and recital 11 thereof?  
(2)      If not, is it contrary to EU law if the national law is interpreted as meaning that information obtained as a result of such authorisation is used to prove the charges brought?’  
35      By letter of 5 August 2022, the Sofiyski gradski sad (Sofia City Court) informed the Court that, following a legislative amendment which entered into force on 27 July 2022, the Spetsializiran nakazatelen sad (Specialised Criminal Court) had been dissolved and that certain criminal cases brought before that court, including the case in the main proceedings, had been transferred to it as from that date.  
   
Consideration of the questions referred  
   
The first question  
36      As a preliminary point, it should be recalled that, when Member States implement, on the basis of Article 15(1) of Directive 2002/58, legislative measures derogating from the principle of confidentiality of electronic communications enshrined in Article 5(1) of that directive, the protection of data subjects falls within the scope of that directive only in so far as the measures at issue impose processing obligations on providers of such communications services, within the meaning of Article 4(2) of Regulation 2016/679, made applicable by Article 2 of Directive 2002/58, read in conjunction with Article 94(2) of that regulation (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 96 and 104 and the case-law cited).  
37      Under the latter provisions, the concept of processing includes, inter alia, for such providers, granting access to communications and data or transmitting them to the competent authorities (see, to that effect and by analogy, judgment of 6 October 2020,   
Privacy International  
, C-623/17, EU:C:2020:790, paragraphs 39 to 41 and the case-law cited).  
38      In the present case, it is for the referring court to ascertain whether the special investigative methods used in the main proceedings and, in particular, the interception referred to in Article 6 of the ZSRS, had the effect of imposing such processing obligations on the providers concerned and whether, therefore, the main proceedings fall within the scope of Directive 2002/58. It must therefore be clarified that the Court will answer the first question only in so far as the case in the main proceedings falls within the scope of that directive, in particular Article 15(1) thereof.  
39      In the light of those preliminary clarifications, it must be held that, by its first question, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of the second paragraph of Article 47 of the Charter, must be interpreted as precluding a national practice under which judicial decisions authorising the use of special investigative methods, following a reasoned request by the criminal authorities, are drawn up in accordance with a pre-drafted text and without individualised reasons, merely stating, apart from the validity period of those authorisations, that the requirements laid down by that legislation, to which those decisions refer, have been complied with.  
40      Article 5(1) of that directive enshrines the principle of the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services. That principle is reflected in the prohibition on listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data without the consent of the users concerned, except in the situations provided for in Article 15(1) of that directive.  
41      The latter article thus provides that Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5 of that directive, in particular when such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society, to ensure the prevention, investigation, detection and prosecution of criminal offences. It also states that all those legislative measures must be in accordance with the general principles of EU law, including the rights, freedoms and principles set out in the Charter.  
42      In that regard, the legislative measures governing access by the competent authorities to the data referred to in Article 5(1) of Directive 2002/58 cannot be confined to requiring that such access serve the purpose pursued by the legislative measures themselves, but must also lay down the substantive and procedural conditions governing that processing (see, to that effect, judgment of 2 March 2021,   
Prokuratuur   
(Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 49 and the case-law cited).  
43      Such measures and conditions must be in accordance with the general principles of EU law, including the principle of proportionality, and with the fundamental rights guaranteed by the Charter, as follows from Article 15(1) of Directive 2002/58, which refers to Article 6(1) and (2) TEU (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 113 and the case-law cited).  
44      In particular, the procedural conditions referred to in paragraph 42 above must be in accordance with the right to a fair trial, enshrined in the second paragraph of Article 47 of the Charter, which corresponds, as is apparent from the explanations relating to that article, to Article 6(1) ECHR. That right requires that all judgments must state the reasons on which they are based (see, to that effect, judgment of 6 September 2012,   
Trade Agency  
, C-619/10, EU:C:2012:531, paragraphs 52 and 53 and the case-law cited).  
45      Therefore, where a legislative measure adopted under Article 15(1) of Directive 2002/58 provides that restrictions to the principle of confidentiality of electronic communications laid down in Article 5(1) of that directive may be adopted by means of judicial decisions, Article 15(1), read in conjunction with the second paragraph of Article 47 of the Charter, requires Member States to provide that such decisions must state the reasons on which they are based.  
46      Indeed, as the Advocate General noted in point 38 of his Opinion, the right to an effective judicial review, guaranteed by Article 47 of the Charter, requires that the person concerned must be able to ascertain the reasons for a decision taken in relation to him or her, either by reading that decision or by being informed of those reasons, so as to enable him or her to defend his or her rights in the best possible conditions and to decide in full knowledge of the facts whether or not to refer the matter to the court with jurisdiction to review the lawfulness of that decision (see, by analogy, judgment of 24 November 2020,   
Minister van Buitenlandse Zaken  
, C-225/19 and C-226/19, EU:C:2020:951, paragraph 43 and the case-law cited).  
47      In the present case, it is apparent from the explanations provided by the referring court that, pursuant to national legislative measures adopted pursuant to Article 15(1) of Directive 2002/58, in particular Article 34 and Article 174(4) of the NPK and Article 15(1) of the ZSRS, read in conjunction with Article 121(4) of the Constitution, reasons must be given for any judicial decision authorising the use of special investigative methods.  
48      That being the case, the first question is raised not in the light of the legislative provisions of the NPK and the ZSRS adopted under Article 15(1) of Directive 2002/58, but of a national judicial practice implementing those legislative provisions, under which decisions to authorise the use of special investigative methods are reasoned by means of a pre-drafted template text intended to cover all possible cases of authorisation, and that does not contain individualised reasons. Such decisions are adopted in a specific procedural context.  
49      It should be noted that, under Bulgarian law, the decision authorising the use of special investigative methods is adopted following a procedure designed to make it possible, with regard to a person in respect of whom there are reasonable grounds to believe that person is preparing, committing or have committed a serious intentional criminal offence, to secure the effective and rapid collection of data which could not be collected by means other than the special investigative methods requested or which could only be collected with extreme difficulty.  
50      In the context of that procedure, the authorities empowered to request the use of such methods, within the meaning of Article 173(1) and (2) of the NPK and Article 13(1) of the ZSRS, must, in accordance with Article 173(2) of the NPK and Article 14(1)(7) of the ZSRS, submit in writing to the court having jurisdiction a reasoned and detailed application setting out the offence which is the subject of the investigation, the measures taken in the context of that investigation and the results thereof, data identifying the person or premises targeted by the application, the operating methods to be applied, the expected duration of the surveillance and the reasons why this duration is requested, as well as the reasons why the use of those methods is essential to the investigation.  
51      It is apparent from the legal rules governing that procedure that the court which grants authorisation to use special investigative methods takes its decision on the basis of a reasoned and detailed application, the content of which, provided for by law, must enable it to ascertain whether the conditions for the grant of such authorisation have been met.  
52      Thus, that practice forms part of legislative measures, adopted under Article 15(1) of Directive 2002/58, which provide for the possibility of taking reasoned judicial decisions which have the effect of restricting the principle of confidentiality of electronic communications and traffic data, laid down in Article 5(1) of that directive. In that regard, it is deemed to implement the obligation to state reasons laid down by those legislative measures in accordance with the requirements of the second paragraph of Article 47 of the Charter referred to in the last sentence of Article 15(1) of that directive with the reference to Article 6(1) and (2) TEU.  
53      In that regard, since, in the context of that procedure, the court having jurisdiction examined the grounds of a detailed application such as that referred to in paragraph 50 of the present judgment, and it considers, at the end of its examination, that that application is justified, it must be held that, by signing a pre-drafted text in accordance with a template indicating that the legal requirements have been complied with, that court endorsed the grounds of the application while ensuring compliance with the legal requirements.  
54      As the European Commission states in its written observations, it would be artificial to require that the authorisation to use special investigative methods should contain a specific and detailed statement of reasons, whereas the application in respect of which that authorisation is granted already contains such a statement of reasons under national law.  
55      On the other hand, once the person concerned has been informed that special investigative methods have been applied to him or her, the obligation to state reasons referred to in the second paragraph of Article 47 of the Charter requires that that person be, in accordance with the case-law referred to in paragraph 46 of the present judgment, in a position to understand the reasons why the use of those methods has been authorised, in order to be able, where appropriate, to challenge that authorisation appropriately and effectively. That requirement also applies to any court, such as, inter alia, the trial court, which, in accordance with its powers, must examine, of its own motion or at the request of the person concerned, the lawfulness of that authorisation.  
56      It will therefore be for the referring court to determine whether, in the context of the practice referred to in paragraph 39 above, compliance with that provision of the Charter and Directive 2002/58 is guaranteed. To that end, it will have to determine whether the person to whom special investigative methods have been applied and the court responsible for reviewing the legality of the authorisation to use those methods are both in a position to understand the reasons for that authorisation.  
57      While that verification is solely a matter for the referring court, the Court, when giving a preliminary ruling on a reference, may, in appropriate cases, nonetheless give clarifications to guide the national court in its decision (judgment of 5 May 2022,   
Victorinox  
, C-179/21, EU:C:2022:353, paragraph 49 and the case-law cited).  
58      In that regard, since authorisation to use special investigative methods is granted on the basis of a reasoned and detailed application from the competent national authorities, it must be verified that the persons referred to in paragraph 56 of the present judgment can have access not only to the authorisation decision but also to the application of the authority which requested that authorisation.  
59      Furthermore, in order to comply with the obligation to state reasons under the second paragraph of Article 47 of the Charter, it is important, as the Advocate General observed, in essence, in point 41 of his Opinion, that those same persons should be able to understand easily and unambiguously, by means of a cross-reading of the authorisation to use special investigative methods and of the accompanying reasoned application, the precise reasons why that authorisation was granted in the light of the factual and legal circumstances characterising the individual case underlying the application, just as it is imperative that such a cross-reading should reveal the validity period of the authorisation.  
60      Where, as in the present case, the authorisation decision merely indicates the validity period of the authorisation and states that the legal provisions to which they refer have been complied with, it is essential that the application should clearly state all the necessary information so that both the person concerned and the court responsible for verifying the legality of the authorisation granted are able to understand that, on the basis of this information alone, the judge who granted the authorisation has, by endorsing the reasoning set out in the application, come to the conclusion that all legal requirements have been met.  
61      If a cross-reading of the application and subsequent authorisation does not make it possible to understand, easily and unequivocally, the reasons for that authorisation, it must be held that the obligation to state reasons which follows from Article 15(1) of Directive 2002/58, read in the light of the second paragraph of Article 47 of the Charter, has not been complied with.  
62      It should also be added that, in accordance with Article 52(3) of the Charter, the rights contained in the Charter have the same meaning and scope as the corresponding rights guaranteed by the ECHR, which does not preclude EU law from affording more extensive protection.  
63      In that regard, it is apparent from the case-law of the European Court of Human Rights that the statement of reasons, albeit succinct, constitutes an essential safeguard against abuse of surveillance in that only such a statement makes it possible to ensure that the judge has correctly examined the application for authorisation and the evidence provided and has genuinely verified whether the surveillance requested constitutes a justified and proportionate interference in the exercise of the right to respect for private and family life guaranteed in Article 8 ECHR. The European Court of Human Rights has nevertheless recognised, with regard to two judgments of the Spetsializiran nakazatelen sad (Specialised Criminal Court), that the lack of individualised reasoning cannot automatically lead to the conclusion that the judge who issued the authorisation did not properly review the application (see, to that effect, ECtHR, 11 January 2022,   
Ekimdzhiev and Others v. Bulgaria  
 (CE:ECHR:2022:0111JUD007007812, §§ 313 and 314 and the case-law cited).  
64      It should also be noted that the judgment of the ECtHR of 15 January 2015,   
Dragojević v. Croatia  
 (CE:ECHR:2015:0115JUD006895511), referred to by the referring court, cannot call into question the considerations set out in paragraphs 58 to 61 of the present judgment. Indeed, in reaching the conclusion that Article 8 ECHR had been infringed, the European Court of Human Rights did not, in that judgment of 15 January 2015, examine the question whether the person concerned could, by a cross-reading of the authorising decisions and the application for surveillance, understand the reasons relied on by the investigating judge, but rather the separate question of whether the lack or inadequacy of the statement of reasons given for the authorising decisions could be remedied a posteriori.  
65      In the light of the foregoing grounds, the answer to the first question is that Article 15(1) of Directive 2002/58, read in the light of the second paragraph of Article 47 of the Charter, must be interpreted as meaning that it does not preclude a national practice under which judicial decisions authorising the use of special investigative methods following a reasoned and detailed application from the criminal authorities, are drawn up by means of a pre-drafted text which does not contain individualised reasons, but which merely states, in addition to the validity period of the authorisation, that the requirements laid down by the legislation to which those decisions refer have been complied with, provided that the precise reasons why the court with jurisdiction considered that the legal requirements had been complied with, in the light of the factual and legal circumstances characterising the case in question, can be easily and unambiguously inferred from a cross-reading of the decision and the application for authorisation, the latter of which must be made accessible, after the authorisation has been given, to the person against whom the use of special investigative methods has been authorised.  
   
The second question  
66      In view of the answer given to the first question, the second question does not require an answer.  
   
Costs  
67      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) read in the light of the second paragraph of Article 47 of the Charter of Fundamental Rights of the European Union,  
is to be interpreted as meaning that it does not preclude a national practice under which judicial decisions authorising the use of special investigative methods following a reasoned and detailed application from the criminal authorities, are drawn up by means of a pre-drafted text which does not contain individualised reasons, but which merely states, in addition to the validity period of the authorisation, that the requirements laid down by the legislation to which those decisions refer have been complied with, provided that the precise reasons why the court with jurisdiction considered that the legal requirements had been complied with, in the light of the factual and legal circumstances characterising the case in question, can be easily and unambiguously inferred from a cross-reading of the decision and the application for authorisation, the latter of which must be made accessible, after the authorisation has been given, to the person against whom the use of special investigative methods has been authorised.

ID: 70660595-e353-4288-a3fb-e5ba004031ed

Judgment of 30 May 2013, C-342/12 (  
Worten  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legal obligation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Security of processing   
   
JUDGMENT OF THE COURT (Third Chamber)  
30 May 2013 (\*)  
(Processing of personal data – Directive 95/46/EC – Article 2 – Concept of ‘personal data’ – Articles 6 and 7 – Principles relating to data quality and criteria for making data processing legitimate – Article 17 – Security of processing – Working time – Record of working time – Access by the national authority responsible for monitoring working conditions – Employer’s obligation to make available the record of working time so as to allow its immediate consultation)  
In Case C-342/12,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Tribunal do trabalho de Viseu (Portugal), made by decision of 13 July 2012, received at the Court on 18 July 2012, in the proceedings  
Worten – Equipamentos para o Lar SA  
v  
Autoridade para as Condições de Trabalho (ACT),  
THE COURT (Third Chamber),  
composed of M. Ilešič, President of the Chamber, E. Jarašiūnas, A. Ó Caoimh (Rapporteur), C. Toader and C.G. Fernlund, Judges,  
Advocate General: J. Kokott,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        Worten   
–   
Equipamentos para o Lar SA, by D. Abrunhosa e Sousa and J. Cruz Ribeiro, advogados,  
–        the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,  
–        the Czech Government, by M. Smolek, acting as Agent,  
–        the Italian Government, by G. Palmieri, acting as Agent, assisted by M. Russo, avvocato dello Stato,  
–        the Hungarian Government, by M. Fehér, K. Szíjjártó and Á. Szilágyi, acting as Agents,  
–        the European Commission, by P. Costa de Oliveira and B. Martenczuk, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2 and Article 17(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Worten – Equipamentos para o Lar SA (‘Worten’), a company established in Viseu (Portugal), and the Autoridade para as Condições de Trabalho (the Authority for Working Conditions; ‘ACT’), concerning ACT’s request to Worten for access to the latter’s record of working time.  
   
Legal context   
   
European Union law  
 Directive 95/46  
3        Under Article 2 of Directive 95/46, headed ‘Definitions’:   
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
...’  
4        Article 3 of that directive, entitled ‘Scope’, is worded as follows:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
5        Article 6 of that directive, which concerns the principles relating to data quality, provides:  
‘1.      Member States shall provide that personal data must be:  
...  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
...  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
6        Article 7 of that directive, which concerns the criteria for making data processing legitimate, states:  
‘Member States shall provide that personal data may be processed only if:  
...  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject; or  
...  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed  
...’  
7        Article 17 of Directive 95/46, entitled ‘Security of processing’, is worded as follows:  
‘1.      Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.  
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.  
...’  
 Directive 2003/88/EC  
8        Under the heading ‘Purpose and scope’, Article 1 of Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time (OJ 2003 L 299, p. 9), provides:  
‘1.      This Directive lays down minimum safety and health requirements for the organisation of working time.  
2.      This Directive applies to:  
(a)      minimum periods of daily rest, weekly rest and annual leave, to breaks and maximum weekly working time ...  
...’  
9        Article 6 of that directive, entitled ‘Maximum weekly working time’, provides:  
‘Member States shall take the measures necessary to ensure that, in keeping with the need to protect the safety and health of workers:  
...  
(b)      the average working time for each seven-day period, including overtime, does not exceed 48 hours.’  
10      Under the first subparagraph of Article 22(1) of that directive:  
‘A Member State shall have the option not to apply Article 6, while respecting the general principles of the protection of the safety and health of workers, and provided it takes the necessary measures to ensure that:  
(a)      no employer requires a worker to work more than 48 hours over a seven-day period … unless he has first obtained the worker’s agreement to perform such work;  
...  
(c)      the employer keeps up-to-date records of all workers who carry out such work;  
(d)      the records are placed at the disposal of the competent authorities, which may, for reasons connected with the safety and/or health of workers, prohibit or restrict the possibility of exceeding the maximum weekly working hours;  
…’  
   
Portuguese legislation  
11      Article 202 of the Employment Code (Codigo do trabalho), approved by Law No 7/2009 of 12 February 2009, provides, under the heading ‘Record of working time’:  
‘(1)      The employer must keep a record of hours worked by workers, including those who are exempt from the normal working hours, in a location that is accessible and in such a way that it can be consulted immediately.   
(2)       That record must set out the times when the working hours begin and end, as well as breaks or periods not included in those working hours, to allow calculation of the number of hours worked by the worker per day and per week ...  
...  
(5)      A breach of the provisions of this article constitutes a serious administrative offence.’  
12      Law No 107/2009 of 14 September 2009 includes, in particular, the following provision:  
‘Article 10 – Inspection procedures  
1.      In the performance of his duties, the employment inspector is to carry out, without prejudice to the provisions of a specific regulation, the following procedures:  
(a)       Request, with immediate effect or with a view to a submission to the decentralised units of the Employment ministry’s inspection services, examine and copy documents and other records relevant for determining the employment relationships and working conditions;   
...  
2.      In the performance of his duties, the social security inspector is to carry out, without prejudice to the provisions of a specific regulation, the following procedures:  
(a)      Request and copy, with immediate effect, for examination, consultation and addition to reports, the books, documents, records, files, and other relevant evidence which belong to the entities whose activity is the subject of the inspection and which are relevant to the verification of the matters inspected;  
...’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
13      On 9 March 2010, ACT carried out an inspection at Worten’s establishment in Viseu, following which it produced a report stating that:  
–        Worten employed four workers in that establishment working on a rotating shift;  
–        the record of working time, setting out the daily work periods, the daily and weekly rest periods and the calculation of the daily and weekly working hours of the workers, was not accessible for immediate consultation;   
–        the workers recorded their working hours by inserting a magnetic card into a time clock installed in the premises of a store located beside the inspected premises;   
–        not only was the record of working time not accessible to any worker of the undertaking or of the establishment where they carried out their duties, but it could also be consulted only by the person who had computerised access to it, namely the regional manager of Worten, who was not present at the time of the inspection; in such a case, only Worten’s central human resources department could provide the data in that register.  
14      On 15 March 2010, in response to a notice to present documents, the record of working time, setting out the legally required data, was submitted to ACT.  
15      By decision of 14 March 2012, ACT found that Warton had committed a serious administrative offence by infringing the rules concerning the record of working time set out in Article 202(1) of the Employment Code, since Warton had not permitted ACT to carry out an immediate consultation, in the establishment concerned, of the record of the working time of the workers employed in that establishment. The serious nature of the offence was stated to arise from the fact that the record of working time allows quick and direct verification of whether the organisation of an undertaking’s activities complies with the regulations concerning working hours. Consequently, ACT imposed a fine of EUR 2 000 on Worten.  
16      Worten brought an action for annulment against that decision before the Tribunal do trabalho de Viseu.  
17      In those circumstances, the Tribunal do trabalho de Viseu decided to stay the proceedings and refer the following question to the Court for a preliminary ruling:  
‘(1)      Is Article 2 of Directive 95/46 … to be interpreted as meaning that the record of working time, that is, the indication, in relation to each worker, of the times when working hours begin and end, as well as the corresponding breaks and intervals, is included within the concept of “personal data”?  
(2)      If so, is the Portuguese State obliged, under Article 17(1) of Directive 95/46 … to provide for appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network?  
(3)      Likewise, if Question 2 is answered in the affirmative, when the Member State does not adopt any measure pursuant to Article 17(1) of Directive 95/46 … and when an employer, as a controller of such data, adopts a system of restricted access to those data which does not allow automatic access by the national authority responsible for monitoring working conditions, is the principle of the primacy of European law to be interpreted as meaning that the Member State cannot penalise that employer for such behaviour?’  
   
Consideration of the questions referred  
   
The first question  
18      By its first question the referring court asks whether Article 2(a) of Directive 95/46 is to be interpreted as meaning that a record of working time, such as that at issue in the main proceedings, containing the indication, in relation to each worker, of the times when working hours begin and end, as well as the corresponding breaks and intervals, constitutes ‘personal data’, within the meaning of that provision.  
19      In that respect, it suffices to note that, as maintained by all of the interested parties who submitted written observations, the data contained in a record of working time such as that at issue in the main proceedings, which concern, in relation to each worker, the daily work periods and rest periods, constitute personal data within the meaning of Article 2(a) of Directive 95/46, because they represent ‘information relating to an identified or identifiable natural person’ (see, to that effect, inter alia, Joined Cases C-465/00, C-138/01 and C-139/01   
Österreichischer Rundfunk and Others  
 [2003] ECR I-4989, paragraph 64; Case C-524/06   
Huber  
 [2008] ECR I-9705, paragraph 43; and Case C-553/07   
Rijkeboer   
[2009] ECR I-3889, paragraph 42).  
20      The collection, recording, organisation, storage, consultation, and use of such data by an employer, as well as their transmission by that employer to the national authorities responsible for monitoring working conditions, thus represent the ‘processing of personal data’ within the meaning of Article 2(b) of Directive 95/46 (see, to that effect, inter alia,   
Österreichischer Rundfunk and Others  
, paragraph 64, and   
Huber  
, paragraph 43).   
21      Moreover, since it is undisputed, in the main proceedings, that the processing of personal data is carried out by automatic means and that none of the exceptions set out in Article 3(2) of Directive 95/46 applies, that processing falls within the scope of Directive 95/46.  
22      Therefore, the answer to the first question is that Article 2(a) of Directive 95/46 is to be interpreted as meaning that a record of working time, such as that at issue in the main proceedings, containing the indication, in relation to each worker, of the times when working hours begin and end, as well as the corresponding breaks and intervals, constitutes ‘personal data’, within the meaning of that provision.  
   
The second and third questions  
23      By its second and third questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 17(1) of Directive 95/46 is to be interpreted as meaning that each Member State is obliged to provide for appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and, if so, whether a Member State which has not adopted such measures may penalise an employer which, as a controller of personal data, has adopted a system of restricted access to those data which does not allow automatic access by the national authority responsible for monitoring working conditions.  
24      It must be recalled that, in accordance with Article 17(1) of Directive 95/46 concerning security of processing, Member States are to provide that the controller must implement appropriate technical and organisational measures which, having regard to the state of the art and the cost of their implementation, are to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected (see, to that effect,   
Rijkeboer  
, paragraph 62).  
25      It follows that, contrary to the premiss on which the second and third questions are based, Article 17(1) of Directive 95/46 does not require Member States, except where they act as controllers, to adopt those technical and organisational measures, as the obligation to adopt such measures concerns solely the controller; namely, in the present case, the employer. Article 17(1) of Directive 95/46 does, however, require the Member States to adopt a provision in their national law providing for that obligation.  
26      Furthermore, it is not in any way apparent from the order for reference that the data at issue in the main proceedings were the subject of accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, or any other unlawful form of processing, within the meaning of Article 17(1) of Directive 95/46. On the contrary, it follows from the information in the file before the Court that it is undisputed, in the main proceedings, that access to those data by the national authority responsible for monitoring working conditions is authorised by national law.  
27      However, in its written observations, Worten claims that the obligation to make available the record of working time so as to allow its immediate consultation, set out in Article 202(1) of the Employment Code, is, in practice, incompatible with the obligation to establish an adequate system of protection of the personal data contained in that record. Such an obligation amounts to allowing any employee of the undertaking concerned to gain access to the personal data contained in that record, in breach of the obligation, set out in Article 17(1) of Directive 95/46, to ensure the security of such data. In Worten’s view, such generalised access therefore renders that provision entirely ineffective.  
28      That line of argument cannot succeed. Contrary to the premiss on which it is based, the obligation for an employer, as a controller of personal data, to provide the national authority responsible for monitoring working conditions immediate access to the record of working time in no way implies that the personal data contained in that record must necessarily, on that ground alone, be made accessible to persons not authorised for that purpose. As the Portuguese government rightly pointed out, all controllers of personal data must, under Article 17(1) of Directive 95/46, implement appropriate technical and organisational measures to ensure that only those persons duly authorised to access the personal data in question are entitled to respond to a request for access from a third party.  
29      Accordingly, it does not appear that Article 17(1) of Directive 95/46 is relevant for the purposes of resolving the dispute in the main proceedings.  
30      However, in the procedure laid down by Article 267 TFEU providing for cooperation between national courts and the Court of Justice, it is for the latter to provide the national court with an answer which will be of use to it and enable it to determine the case before it. To that end, the Court may have to reformulate the questions referred to it. The Court has a duty to interpret all provisions of European Union law which national courts require in order to decide the actions pending before them, even if those provisions are not expressly indicated in the questions referred to the Court of Justice by those courts (see, to that effect, inter alia, Case C-45/06   
Campina   
[2007] ECR I-2089, paragraphs 30 and 31, and Case C-243/09   
Fuß  
 [2010] ECR I-9849, paragraph 39).  
31      Consequently, even if, formally, the referring court has limited its questions to the interpretation of Article 17(1) of Directive 95/46, that does not prevent this Court from providing the referring court with all the elements of interpretation of European Union law that may be of assistance in adjudicating in the case pending before it, whether or not the referring court has referred to them in the wording of its questions. It is, in this regard, for the Court to extract from all the information provided by the national court, in particular from the grounds of the decision to make the reference, the points of European Union law which require interpretation in view of the subject-matter of the dispute (see   
Fuß  
, paragraph 40).  
32      In the present case, it is clear from the documents before the Court that the referring court seeks, in essence, to determine whether the provisions of Directive 95/46 are to be interpreted as precluding national legislation, such as that at issue in the main proceedings, which requires an employer to make the record of working time available to the national authority responsible for monitoring working conditions so as to allow its immediate consultation. As noted in paragraph 15 of the present judgment, the breach of that obligation laid down in Article 202(1) of the Employment Code was the reason for the fine imposed on Worten.  
33      It should be recalled that, in accordance with the provisions of Chapter II of Directive 95/46, entitled ‘General rules on the lawfulness of the processing of personal data’, all processing of personal data must, subject to the exceptions permitted under Article 13, comply, first, with the principles relating to data quality set out in Article 6 of Directive 95/46 and, secondly, with one of the six principles for making data processing legitimate listed in Article 7 of that directive (  
Österreichischer Rundfunk and Others  
, paragraph 65;   
Huber  
, paragraph 48; and Joined Cases C-468/10 and C-469/10   
ANSEF and FECEMD  
 [2011] ECR I-12181, paragraph 26).   
34      More specifically, under Article 6(1)(b) and (c) of Directive 95/46, the data must be ‘collected for specified, explicit and legitimate purposes’ and must be ‘adequate, relevant and not excessive’ in relation to those purposes. In addition, under Article 7(c) and (e) of the directive, the processing of personal data is permissible only if it ‘is necessary for compliance with a legal obligation to which the controller is subject’ or ‘is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed’ (  
Österreichischer Rundfunk and Others  
, paragraph 66).  
35      That seems to be the case in a situation such as that in the main proceedings, since it appears that – which is for the referring court to verify – on the one hand, the personal data contained in the record of working time are collected in order to ensure compliance with the legislation relating to working conditions and, on the other hand, the processing of those personal data is necessary for compliance with a legal obligation to which the employer is subject and to the performance of the monitoring task entrusted to the national authority responsible for monitoring working conditions.  
36      As regards the actual rules for the organisation of the national authority’s access to those personal data in order to carry out its task of monitoring working conditions, it must be recalled that only the grant of access to authorities having powers in that field could be considered to be necessary within the meaning of Article 7(e) of Directive 95/46 (see, to that effect,   
Huber  
, paragraph 61).  
37      Concerning the employer’s obligation to provide that national authority immediate access to the record of working time, it is clear from the case-law that such an obligation could be necessary, within the meaning of Article 7(e) of Directive 95/46, if it contributes to the more effective application of the legislation relating to working conditions (see, by analogy,   
Huber  
, paragraph 62).  
38      In that respect, it must be pointed out that the purpose of Directive 2003/88 is to lay down minimum requirements intended to improve the living and working conditions of workers through approximation of national rules concerning, in particular, the duration of working time, by ensuring that they are entitled to minimum rest periods – particularly daily and weekly – and adequate breaks and by providing for a ceiling on the average duration of the working week (see, to that effect, inter alia, Joined Cases C-397/01 to C-403/01   
Pfeiffer and Others  
 [2004] ECR I-8835, paragraph 76, and Case C-429/09   
Fuß  
 [2010] ECR I-12167, paragraph 43).  
39      In view of the above, Article 6(b) of Directive 2003/88 requires the Member States to take the ‘measures necessary’ to ensure that, in keeping with the need to protect the safety and health of workers, the average working time for each seven-day period, including overtime, does not exceed 48 hours (see, to that effect,   
Pfeiffer and Others  
, paragraph 100, and Case C-243/09   
Fuß  
, paragraph 33).  
40      Moreover, the first subparagraph of Article 22(1) of Directive 2003/88 provides that a Member State may choose not to apply Article 6 of that directive, provided, inter alia, it takes the necessary measures to ensure that the employer keeps up-to-date records of all workers who carry out such work (point (c) of the first subparagraph of Article 22(1) of that directive) and that the records are placed at the disposal of the competent authorities, which may, for reasons connected with the safety and/or health of workers, prohibit or restrict the possibility of exceeding the maximum weekly working hours (point (d) of subparagraph 1 of Article 22(1) of that directive).  
41      According to the European Commission, although Directive 2003/88 does not expressly require the Member States to adopt legislation such as that at issue in the main proceedings, the monitoring of compliance with the obligations imposed by that directive may entail – as ‘measures necessary’ to the performance of the objectives which that directive pursues – the establishment of surveillance measures. In the Commission’s view, the employer’s obligation to allow immediate consultation of the record of working time ensures that data is not altered during the interval between the inspection visit carried out by the competent national authorities and the actual verification of those data by those authorities.  
42      Worten claims, by contrast, that this obligation is excessive, given the interference it entails in workers’ private lives. First, the record of working time is intended to provide workers with a means of proving the hours they have actually worked. The authenticity of that record has not been contested in the main proceedings. Secondly, that record allows the assessment of average working times, for the purposes of monitoring, inter alia, working hours exemptions. For that purpose, the immediate availability of those records does not, according to Worten, provide any added value. Moreover, the information in that record could be submitted subsequently.  
43      In the present case, it is for the referring court to examine whether the employer’s obligation to provide the competent national authority access to the record of working time so as to allow its immediate consultation can be considered necessary for the purposes of the performance by that authority of its monitoring task, by contributing to the more effective application of the legislation relating to working conditions, in particular as regard working time.  
44      In that respect, it must also be noted that, in any case, if such an obligation is considered necessary to achieving that objective, the penalties imposed with a view to ensuring the effective application of the requirements laid down by Directive 2003/88 must also respect the principle of proportionality, which it is also for the referring court to verify in the main proceedings (see, by analogy, Case C-101/01   
Lindqvist  
 [2003] ECR I-12971, paragraph 88).  
45      Consequently, the answer to the second and third questions is that Article 6(1)(b) and (c) and Article 7(c) and (e) of Directive 95/46 do not preclude national legislation, such as that at issue in the main proceedings, which requires an employer to make a record of working time available to the national authority responsible for monitoring working conditions so as to allow its immediate consultation, provided that this obligation is necessary for the purposes of the performance by that authority of its task of monitoring the application of the legislation relating to working conditions, in particular as regards working time.  
   
Costs  
46      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is to be interpreted as meaning that a record of working time, such as that at issue in the main proceedings, which indicates, in relation to each worker, the times when working hours begin and end, as well as the corresponding breaks and intervals, is included within the concept of ‘personal data’, within the meaning of that provision.  
2.        
Article 6(1)(b) and (c) and Article 7(c) and (e) of Directive 95/46 do not preclude national legislation, such as that at issue in the main proceedings, which requires an employer to make the record of working time available to the national authority responsible for monitoring working conditions so as to allow its immediate consultation, provided that this obligation is necessary for the purposes of the performance by that authority of its task of monitoring the application of the legislation relating to working conditions, in particular as regards working time.

ID: 72f7ce98-df48-43df-8040-218b933c2a58

Judgment of 4 May 2017, C-13/16 (  
Rīgas satiksme  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
   
JUDGMENT OF THE COURT (Second Chamber)  
4 May 2017 (\*)  
(Reference for a preliminary ruling — Directive 95/46/EC — Article 7(f) — Personal data — Conditions for the lawful processing of personal data — Concept of ‘necessity for the realisation of the legitimate interests of a third party’ — Request for disclosure of personal data of a person responsible for a road accident in order to exercise a legal claim — Obligation on the controller to grant such a request — No such obligation)  
In Case C-13/16,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Augstākās tiesas, Administratīvo lietu departaments (Supreme Court, Administrative Division, Latvia), made by decision of 30 December 2015, received at the Court on 8 January 2016, in the proceedings  
Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde  
v  
Rīgas pašvaldības SIA ‘Rīgas satiksme’,  
THE COURT (Second Chamber),  
composed of M. Ilešič, President of the Chamber, A. Prechal, A. Rosas (Rapporteur), C. Toader and E. Jarašiūnas, Judges,  
Advocate General : M. Bobek,  
Registrar: M. Aleksejev, Administrator,  
having regard to the written procedure and further to the hearing on 24 November 2016,  
after considering the observations submitted on behalf of:  
–        Rīgas pašvaldības SIA ‘Rīgas satiksme’ by L. Bemhens, acting as Agent,  
–        the Latvian Government, by I. Kalniņš and by A. Bogdanova, acting as Agents,  
–        the Czech Government, by J. Vláčil and M. Smolek, acting as Agents,  
–        the Spanish Government, by M.J. García-Valdecasas Dorrego, acting as Agent,  
–        the Austrian Government, by G. Eberhard, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes and M. Figueiredo and by C. Vieira Guerra, acting as Agents,  
–        the European Commission, by D. Nardi and H. Kranenborg and by I. Rubene, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 26 January 2017,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 7(f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde (Office responsible for road traffic administrative infringements of the Security Police of the Region of Riga, Latvia) (‘the national police’) and Rīgas pašvaldības SIA ‘Rīgas satiksme’ (‘Rīgas satiksme’), a trolleybus company in the city of Riga, relating to a request for disclosure of data identifying the perpetrator of an accident.  
   
Legal context  
   
EU law  
3        Article 1 of Directive 95/46, entitled ‘Object of the Directive’, provides:  
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
4        Article 2 of that directive provides:  
‘For the purpose of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;  
…’  
5        Article 5 of Directive 95/46 states:  
‘Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.’  
6        In Section II, entitled ‘Criteria for making data processing legitimate’, of Chapter II of Directive 95/46, Article 7 provides:  
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent; or  
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject; or  
(d)      processing is necessary in order to protect the vital interests of the data subject; or  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
7        Article 8(2)(e) of Directive 95/46 provides that the prohibition on the processing of certain types of personal data, such as that revealing racial origin or political opinions, is not to apply where the processing relates to data which is manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.  
   
Latvian law  
8        Article 6 of the Fizisko personu datu aizsardzības likums (Law on the protection of personal data), of 23 March 2000 (  
Latvijas Vēstnesis,   
2000  
,  
 No 123/124), provides:  
‘Everyone has the right to the protection of personal data concerning him or her.’  
9        Article 7 of that law, which seeks to transpose Article 7 of Directive 95/46, provides that the processing of personal data is to be authorised only if that law does not provide otherwise and if at least one of the following requirements is met:  
‘(1) the data subject has given his consent;  
(2)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;  
(3)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
(4)      processing is necessary in order to protect the vital interests of the data subject, including his life and health;  
(5)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;  
(6)      processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.’  
10      Article 12 of that Law provides that personal data relating to criminal offenses, criminal and administrative convictions, as well as judicial decisions or judicial case files, may be processed only by persons provided for by law and in the cases provided for by law.  
11      According to Article 261 of the Latvijas Administratīvo pārkāpumu kodekss (Latvian Administrative Infringements Code), a person who has suffered harm caused by an infringement may be given the status of victim in the context of administrative proceedings leading to sanctions, by the body or official who is authorised to examine the case. That provision provides for the rights of victims, including the right to consult the case file and to use his procedural rights to obtain compensation.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
12      In December 2012 a road accident occurred in Riga. A taxi driver had stopped his vehicle at the side of the road. As a trolleybus of Rīgas satiksme was passing alongside the taxi, a passenger sitting in the back seat of that taxi opened the door, which scraped against and damaged the trolleybus. Administrative proceedings leading to sanctions were initiated and a report was drawn up finding an administrative offence.  
13      As the taxi driver was initially held responsible for that accident, Rīgas satiksme sought compensation from the insurance company covering the civil liability of the owner and lawful user of the taxi. However, that insurance company informed Rīgas satiksme that it would not pay Rīgas satiksme any compensation on the basis that the accident had occurred due to the conduct of the passenger in that taxi, rather than the driver. It stated that Rīgas satiksme could bring civil proceedings against that passenger.  
14      Rīgas satiksme then applied to the national police asking it to provide information concerning the person on whom an administrative penalty had been imposed following the accident, to provide copies of the statements given by the taxi driver and the passenger on the circumstances of the accident, and to indicate the first name and surname, identity document number, and address of the taxi passenger. Rīgas satiksme indicated to the national police that the information requested would be used only for the purpose of bringing civil proceedings.  
15      The national police responded by granting Rīgas satiksme’s request in part, namely by providing the first name and surname of the taxi passenger but refusing to provide the identity document number and address of that person. Nor did it send Rīgas satiksme the statements given by the persons involved in the accident.  
16      The decision of the national police was based on the fact that documents in the case file in administrative proceedings leading to sanctions may be provided only to the parties to those proceedings. Rīgas satiksme is not a party to the case at issue. Under the Latvian Administrative Infringements Code, a person may at his express request be given the status of victim in administrative proceedings leading to sanctions by the body or official responsible for examining the case. In the present case Rīgas satiksme did not exercise that right.  
17      Rīgas satiksme brought an administrative law action before the administratīvā rajona tiesa (District Administrative Court, Latvia) against the decision of the national police in so far as it refused to reveal the identity document number and address of the passenger involved in the accident. By judgment of 16 May 2014, that court upheld the action brought by Rīgas satiksme and ordered the national police to provide the information relating to the identity document number and place of residence of that passenger.  
18      The national police brought an appeal in cassation before the referring court. That court sought an opinion from the Datu valsts inspekcija (National Data Protection Agency, Latvia) the Data Protection Agency which stated, in its response of 13 October 2015, that Article 7(6) of the Law on the Protection of Personal Data could not be used as a legal basis to provide personal data in the case in the main proceedings as the Latvian Administrative Infringements Code sets out the persons to which the national police may disclose the information relating to a case. Consequently, according to the National Data Protection Agency, the disclosure of personal data relating to administrative proceedings leading to sanctions may be carried out only in accordance with paragraphs 3 and 5 of that article in the situations laid down by the law. Article 7 of the law does not oblige the data controller, in this case, the national police, to process the data, but simply permits it.  
19      The National Data Protection Agency also indicated that Rīgas satiksme had two other means of obtaining that information. It could either submit a reasoned request to the Civil Registry or apply to the courts pursuant to Articles 98 to 100 of the Latvian Law on Civil Procedure for the production of evidence, in order for the court in question to request from the national police the personal data so that Rīgas satiksme would be able to bring proceedings against the person concerned.  
20      The referring court has doubts regarding the effectiveness of the means of obtaining the personal data referred to by the National Data Protection Agency. It states, in that regard, first, that if an application made to the Civil Registry mentions only the name of the taxi passenger, it may be that that passenger cannot be identified by his identity document number as the same surname and first name may be shared by several people. Second, the referring court takes the view that, in the light of the national law on the provision on evidence, in order to bring a civil action, the applicant would have to know at least the place of residence of the defendant.  
21      In that regard, the referring court is of the opinion that there are doubts as to the interpretation of the concept of ‘necessity’ referred to in Article 7(f) of that directive.  
22      In those circumstances, the Augstākās tiesas Administratīvo lietu departaments (Supreme Court, Administrative Division, Latvia) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must the phrase ‘is necessary for the purposes of the legitimate interests pursued by the … third party or parties to whom the data are disclosed’, in Article 7(f) of Directive 95/46/EC, be interpreted as meaning that the national police must disclose to Rīgas satiksme the personal data sought [by the latter] which are necessary in order for civil proceedings to be initiated?  
(2)      Is the fact that, as the documents in the case file indicate, the taxi passenger whose data is sought by Rīgas satiksme was a minor at the time of the accident relevant to the answer to that question?’  
   
Consideration of the questions referred  
23      By its questions, which it is appropriate to examine together, the referring court asks whether Article 7(f) of Directive 95/46 must be interpreted as imposing the obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data, and if the fact that that person is a minor has a bearing on the interpretation of that provision.  
24      In the case in the main proceedings, it is common ground that the identity document number and the address of the taxi passenger, of which Rīgas satiksme requests communication, constitute information concerning an identified or identifiable natural person and, therefore, ‘personal data’ within the meaning of Article 2(a) of Directive 95/46. It is also common ground that the national police, to which that request was addressed, is responsible for processing that data and, in particular, for their possible communication within the meaning of Article 2(d) of that directive.  
25      In accordance with Article 5 of Directive 95/46, it is for the Member States to specify, within the limits of the provisions of that directive, the conditions under which the processing of personal data is lawful. Article 7 of that directive, which lays down the principles relating to the legitimacy of such processing, provides in that regard that ‘Member States shall provide that [it] may be processed only if’ one of the situations listed exhaustively by that provision exists. Under Article 7(f), such processing may be carried out where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1) of Directive 95/46.  
26      It is accordingly clear from the scheme of Directive 95/46 and from the wording of Article 7 thereof that Article 7(f) of Directive 95/46 does not, in itself, set out an obligation, but expresses the possibility of processing data such as the communication to a third party of data necessary for the purposes of the legitimate interests pursued by that third party. As the Advocate General stated in points 43 to 46 of his Opinion, such an interpretation may also be deduced from other EU instruments touching upon personal data (see, to that effect, as regards the processing of personal data in the electronic communications sector, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraphs 54 and 55).  
27      However, it should be pointed out that Article 7(f) of Directive 95/46 does not preclude such communication, in the event that it is made on the basis of national law, in accordance with the conditions laid down in that provision.  
28      In that regard, Article 7(f) of Directive 95/46 lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.  
29      As regards the condition relating to the pursuit of a legitimate interest, as the Advocate General stated in points 65, 79 and 80 of his Opinion, there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 53). That analysis is supported by Article 8(2)(e) of Directive 95/46, which provides that the prohibition on the processing of certain types of personal data, such as those revealing racial origin or political opinions, is not to apply, in particular, where the processing is necessary for the establishment, exercise or defence of legal claims.  
30      As regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (judgments of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 86; of 7 November 2013,   
IPI  
, C-473/12, EU:C:2013:715, paragraph 39; and of 11 December 2014,   
Ryneš  
, C-212/13, EU:C:2014:2428, paragraph 28). In that regard, according to the information provided by the national court, communication of merely the first name and surname of the person who caused the damage does not make it possible to identify that person with sufficient precision in order to be able to bring an action against him. Accordingly, for that purpose, it is necessary to obtain also the address and/or the identification number of that person.  
31      Finally, as regards the condition of balancing the opposing rights and interests at issue, it depends in principle on the specific circumstances of the particular case (see, to that effect, judgments of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 40, and of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 62).  
32      In that regard, the Court has held that it is possible to take into consideration the fact that the seriousness of the infringement of the data subject’s fundamental rights resulting from that processing can vary depending on the possibility of accessing the data at issue in public sources (see, to that effect, judgment of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 44).  
33      As regards the second part of the question referred for a preliminary ruling as set out in paragraph 23 of the present judgment, it should be noted that the age of the data subject may be one of the factors which should be taken into account in the context of that balancing of interests. However, as the Advocate General pointed out in points 82 to 84 of his Opinion and subject to the determination to be carried out in that respect by the national court, it does not appear to be justified, in circumstances such as those at issue in the main proceedings, to refuse to disclose to an injured party the personal data necessary for bringing an action for damages against the person who caused the harm, or, where appropriate, the persons exercising parental authority, on the ground that the person who caused the damage was a minor.  
34      It follows from the foregoing considerations that Article 7(f) of Directive 95/46 must be interpreted as not imposing the obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data. However, Article 7(f) of that directive does not preclude such disclosure on the basis of national law.  
   
Costs  
35      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
Article 7(f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as not imposing the obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data. However, Article 7(f) of that directive does not preclude such disclosure on the basis of national law.

ID: 769f3b79-0b27-400c-8431-5cf94b7f40af

Judgment of 8 Apr 2014, C-293/12 (  
Digital Rights Ireland and Seitlinger and Others  
)  
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Confidentiality of electronic communications   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
E-privacy Directive   
 >   
Electronic communications   
 >   
Data retention and access of national authorities   
Data Retention Directive   
   
JUDGMENT OF THE COURT (Grand Chamber)  
8 April 2014 (\*)  
(Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)  
In Joined Cases C-293/12 and C-594/12,  
REQUESTS for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, received at the Court on 11 June and 19 December 2012, in the proceedings  
Digital Rights Ireland Ltd  
 (C-293/12)  
v  
Minister for Communications, Marine and Natural Resources,  
Minister for Justice, Equality and Law Reform,  
Commissioner of the Garda Síochána,  
Ireland,  
The Attorney General,  
intervener:  
Irish Human Rights Commission,   
and  
Kärntner Landesregierung   
(C-594/12),  
Michael Seitlinger,  
Christof Tschohl and others,   
THE COURT (Grand Chamber),  
composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), E. Juhász, A. Borg Barthet, C.G. Fernlund and J.L. da Cruz Vilaça, Presidents of Chambers, A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, C. Toader and C. Vajda, Judges,  
Advocate General: P. Cruz Villalón,  
Registrar: K. Malacek, Administrator,  
having regard to the written procedure and further to the hearing on 9 July 2013,  
after considering the observations submitted on behalf of:  
–        Digital Rights Ireland Ltd, by F. Callanan, Senior Counsel, and F. Crehan, Barrister-at-Law, instructed by S. McGarr, Solicitor,  
–        Mr Seitlinger, by G. Otto, Rechtsanwalt,  
–        Mr Tschohl and Others, by E. Scheucher, Rechtsanwalt,  
–        the Irish Human Rights Commission, by P. Dillon Malone, Barrister-at-Law, instructed by S. Lucey, Solicitor,  
–        Ireland, by E. Creedon and D. McGuinness, acting as Agents, assisted by E. Regan, Senior Counsel, and D. Fennelly, Barrister-at-Law,  
–        the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,   
–        the Spanish Government, by N. Díaz Abad, acting as Agent,  
–        the French Government, by G. de Bergues and D. Colas and by B. Beaupère-Manokha, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, assisted by A. De Stefano, avvocato dello Stato,  
–        the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,   
–        the United Kingdom Government, by L. Christie, acting as Agent, assisted by S. Lee, Barrister,  
–        the European Parliament, by U. Rösslein and A. Caiola and by K. Zejdová, acting as Agents,  
–        the Council of the European Union, by J. Monteiro and E. Sitbon and by I. Šulce, acting as Agents,  
–        the European Commission, by D. Maidani, B. Martenczuk and M. Wilderspin, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 12 December 2013,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern the validity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).  
2        The request made by the High Court (Case C-293/12) concerns proceedings between (i) Digital Rights Ireland Ltd. (‘Digital Rights’) and (ii) the Minister for Communications, Marine and Natural Resources, the Minister for Justice, Equality and Law Reform, the Commissioner of the Garda Síochána, Ireland and the Attorney General, regarding the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications.   
3        The request made by the Verfassungsgerichtshof (Constitutional Court) (Case C-594/12) concerns constitutional actions brought before that court by the Kärntner Landesregierung (Government of the Province of Carinthia) and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants regarding the compatibility with the Federal Constitutional Law (Bundes-Verfassungsgesetz) of the law transposing Directive 2006/24 into Austrian national law.  
   
Legal context  
   
Directive 95/46/EC  
4        The object of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), according to Article 1(1) thereof, is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with regard to the processing of personal data.   
5        As regards the security of processing such data, Article 17(1) of that directive provides:  
‘Member States shall provide that the controller must implement appropriate technical and organi[s]ational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.   
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.’   
   
Directive 2002/58/EC  
6        The aim of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11, ‘Directive 2002/58), according to Article 1(1) thereof, is to harmonise the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and to confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the European Union. According to Article 1(2), the provisions of that directive particularise and complement Directive 95/46 for the purposes mentioned in Article 1(1).   
7        As regards the security of data processing, Article 4 of Directive 2002/58 provides:  
‘1.      The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.  
1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:  
–        ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,  
–        protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,  
–        ensure the implementation of a security policy with respect to the processing of personal data,   
Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.  
2.      In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.’   
8        As regards the confidentiality of the communications and of the traffic data, Article 5(1) and (3) of that directive provide:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
…  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
9        Article 6(1) of Directive 2002/58 states:  
‘Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).’  
10      Article 15 of Directive 2002/58 states in paragraph 1:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’  
   
Directive 2006/24  
11      After having launched a consultation with representatives of law enforcement authorities, the electronic communications industry and data protection experts, on 21 September 2005 the Commission presented an impact assessment of policy options in relation to the rules on the retention of traffic data (‘the impact assessment’). That assessment served as the basis for the drawing up of the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final, ‘the proposal for a directive’), also presented on 21 September 2005, which led to the adoption of Directive 2006/24 on the basis of Article 95 EC.  
12      Recital 4 in the preamble to Directive 2006/24 states:  
‘Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.’  
13      According to the first sentence of recital 5 in the preamble to Directive 2006/24, ‘[s]everal Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences’.  
14      Recitals 7 to 11 in the preamble to Directive 2006/24 read as follows:  
‘(7)       The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.  
(8)       The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.   
(9)      Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) [signed in Rome on 4 November 1950], everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. …  
(10)      On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.   
(11)      Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.’  
15      Recitals 16, 21 and 22 in the preamble to Directive 2006/24 state:  
‘(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.  
(21)  Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.  
(22)  This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.’  
16      Directive 2006/24 lays down the obligation on the providers of publicly available electronic communications services or of public communications networks to retain certain data which are generated or processed by them. In that context, Articles 1 to 9, 11 and 13 of the directive state:  
‘Article 1  
Subject matter and scope  
1.      This Directive aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.  
2.      This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.  
Article 2  
Definitions  
1.      For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) …, and in Directive 2002/58/EC shall apply.  
2.      For the purpose of this Directive:  
(a)      “data” means traffic data and location data and the related data necessary to identify the subscriber or user;  
(b)      “user” means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;  
(c)      “telephone service” means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);  
(d)      “user ID” means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;   
(e)      “cell ID” means the identity of the cell from which a mobile telephony call originated or in which it terminated;  
(f)      “unsuccessful call attempt” means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.  
Article 3  
Obligation to retain data  
1.      By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.  
2.      The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.  
Article 4  
Access to data  
Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of EU law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.  
Article 5  
Categories of data to be retained  
1.      Member States shall ensure that the following categories of data are retained under this Directive:  
(a)      data necessary to trace and identify the source of a communication:  
(1)      concerning fixed network telephony and mobile telephony:  
(i)      the calling telephone number;  
(ii)      the name and address of the subscriber or registered user;  
(2)      concerning Internet access, Internet e-mail and Internet telephony:  
(i)      the user ID(s) allocated;  
(ii)      the user ID and telephone number allocated to any communication entering the public telephone network;  
(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;  
(b)      data necessary to identify the destination of a communication:  
(1)      concerning fixed network telephony and mobile telephony:  
(i)      the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;  
(ii)      the name(s) and address(es) of the subscriber(s) or registered user(s);  
(2)      concerning Internet e-mail and Internet telephony:  
(i)      the user ID or telephone number of the intended recipient(s) of an Internet telephony call;  
(ii)      the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;  
(c)      data necessary to identify the date, time and duration of a communication:  
(1)      concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;  
(2)      concerning Internet access, Internet e-mail and Internet telephony:  
(i)      the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;  
(ii)      the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;  
(d)      data necessary to identify the type of communication:  
(1)      concerning fixed network telephony and mobile telephony: the telephone service used;  
(2)      concerning Internet e-mail and Internet telephony: the Internet service used;  
(e)      data necessary to identify users’ communication equipment or what purports to be their equipment:  
(1)      concerning fixed network telephony, the calling and called telephone numbers;  
(2)      concerning mobile telephony:  
(i)      the calling and called telephone numbers;  
(ii)      the International Mobile Subscriber Identity (IMSI) of the calling party;  
(iii) the International Mobile Equipment Identity (IMEI) of the calling party;  
(iv)      the IMSI of the called party;  
(v)      the IMEI of the called party;  
(vi)      in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;  
3)      concerning Internet access, Internet e-mail and Internet telephony:  
(i)      the calling telephone number for dial-up access;  
(ii)      the digital subscriber line (DSL) or other end point of the originator of the communication;  
(f)      data necessary to identify the location of mobile communication equipment:  
(1)      the location label (Cell ID) at the start of the communication;  
(2)      data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.  
2.      No data revealing the content of the communication may be retained pursuant to this Directive.  
Article 6  
Periods of retention  
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.  
Article 7  
Data protection and data security  
Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:  
(a)      the retained data shall be of the same quality and subject to the same security and protection as those data on the network;  
(b)      the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;  
(c)      the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;  
and  
(d)      the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.  
Article 8  
Storage requirements for retained data  
Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.  
Article 9  
Supervisory authority  
1.      Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.  
2.      The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.  
…  
Article 11  
Amendment of Directive 2002/58/EC  
The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:  
“1a. Paragraph 1 shall not apply to data specifically required by [Directive 2006/24/EC] to be retained for the purposes referred to in Article 1(1) of that Directive.”  
…  
Article 13  
Remedies, liability and penalties  
1.      Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.  
2.      Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.’  
   
The actions in the main proceedings and the questions referred for a preliminary ruling  
   
Case C-293/12  
17      On 11 August 2006, Digital Rights brought an action before the High Court in which it claimed that it owned a mobile phone which had been registered on 3 June 2006 and that it had used that mobile phone since that date. It challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications and asked the national court, in particular, to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State.   
18      The High Court, considering that it was not able to resolve the questions raised relating to national law unless the validity of Directive 2006/24 had first been examined, decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:   
‘1.      Is the restriction on the rights of the [p]laintiff in respect of its use of mobile telephony arising from the requirements of Articles 3, 4 … and 6 of Directive 2006/24/EC incompatible with [Article 5(4)] TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of:  
(a)      Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime?  
and/or  
(b)      Ensuring the proper functioning of the internal market of the European Union?  
2.      Specifically,  
(i)      Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU?  
(ii)      Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union (“the Charter”)] and Article 8 ECHR?  
(iii) Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?  
(iv)      Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?  
(v)      Is Directive 2006/24 compatible with the right to [g]ood [a]dministration laid down in Article 41 of the Charter?  
3.      To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess, the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the [Charter], including Article 7 thereof (as informed by Article 8 of the ECHR)?’   
   
Case C–594/12  
19      The origin of the request for a preliminary ruling in Case C-594/12 lies in several actions brought before the Verfassungsgerichtshof by the Kärntner Landesregierung and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants, respectively, seeking the annulment of Paragraph 102a of the 2003 Law on telecommunications (Telekommunikationsgesetz 2003), which was inserted into that 2003 Law by the federal law amending it (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl I, 27/2011) for the purpose of transposing Directive 2006/24 into Austrian national law. They take the view, inter alia, that Article 102a of the Telekommunikationsgesetz 2003 infringes the fundamental right of individuals to the protection of their data.   
20      The Verfassungsgerichtshof wonders, in particular, whether Directive 2006/24 is compatible with the Charter in so far as it allows the storing of many types of data in relation to an unlimited number of persons for a long time. The Verfassungsgerichtshof takes the view that the retention of data affects almost exclusively persons whose conduct in no way justifies the retention of data relating to them. Those persons are exposed to a greater risk that authorities will investigate the data relating to them, become acquainted with the content of those data, find out about their private lives and use those data for multiple purposes, having regard in particular to the unquantifiable number of persons having access to the data for a minimum period of six months. According to the referring court, there are doubts as to whether that directive is able to achieve the objectives which it pursues and as to the proportionality of the interference with the fundamental rights concerned.   
21      In those circumstances the Verfassungsgerichtshof decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘1.      Concerning the validity of acts of institutions of the European Union:  
Are Articles 3 to 9 of [Directive 2006/24] compatible with Articles 7, 8 and 11 of the [Charter]?  
2.      Concerning the interpretation of the Treaties:  
(a)      In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Verfassungsgerichtshof, must [Directive 95/46] and Regulation (EC) No 45/2001 of the European Parliament and of the Council [of 18 December 2000] on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [OJ 2001 L 8, p. 1] be taken into account, for the purposes of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?  
(b)      What is the relationship between “Union law”, as referred to in the final sentence of Article 52(3) of the Charter, and the directives in the field of the law on data protection?  
(c)      In view of the fact that [Directive 95/26] and Regulation … No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?  
(d)      Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?  
(e)      Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the [ECHR], can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter article?’  
22      By decision of the President of the Court of 11 June 2013, Cases C-293/12 and C-594/12 were joined for the purposes of the oral procedure and the judgment.   
   
Consideration of the questions referred  
   
The second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12  
23      By the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, which should be examined together, the referring courts are essentially asking the Court to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter.   
 The relevance of Articles 7, 8 and 11 of the Charter with regard to the question of the validity of Directive 2006/24  
24      It follows from Article 1 and recitals 4, 5, 7 to 11, 21 and 22 of Directive 2006/24 that the main objective of that directive is to harmonise Member States’ provisions concerning the retention, by providers of publicly available electronic communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter.  
25      The obligation, under Article 3 of Directive 2006/24, on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raises questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter.   
26      In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users’ communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.   
27      Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.   
28      In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.   
29      The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (Cases C-92/09 and C-93/09   
Volker und Markus Schecke and Eifert   
EU:C:2010:662, paragraph 47).  
30      Whereas the references for a preliminary ruling in the present cases raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter.   
31      In the light of the foregoing considerations, it is appropriate, for the purposes of answering the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, to examine the validity of the directive in the light of Articles 7 and 8 of the Charter.  
 Interference with the rights laid down in Articles 7 and 8 of the Charter  
32      By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, as the Advocate General has pointed out, in particular, in paragraphs 39 and 40 of his Opinion, derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.   
33      To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C-465/00, C-138/01 and C-139/01   
Österreichischer Rundfunk and Others   
EU:C:2003:294, paragraph 75).   
34      As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person’s private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.   
35      Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R.,   
Leander v. Sweden  
, 26 March 1987, § 48, Series A no 116;   
Rotaru v. Romania   
[GC], no. 28341/95, § 46, ECHR 2000-V; and   
Weber and Saravia v. Germany  
 (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.   
36      Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.  
37      It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.   
 Justification of the interference with the rights guaranteed by Articles 7 and 8 of the Charter  
38      Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.   
39      So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.  
40      Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.  
41      As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States’ provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.  
42      It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest (see, to that effect, Cases C-402/05 P and C-415/05 P   
Kadi and Al Barakaat International Foundation  
 v   
Council and Commission  
 EU:C:2008:461, paragraph 363, and Cases C-539/10 P and C-550/10 P   
Al-Aqsa  
 v   
Council  
 EU:C:2012:711, paragraph 130). The same is true of the fight against serious crime in order to ensure public security (see, to that effect, Case C-145/09   
Tsakouridis   
EU:C:2010:708, paragraphs 46 and 47). Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.   
43      In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.   
44      It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.  
45      In those circumstances, it is necessary to verify the proportionality of the interference found to exist.  
46      In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (see, to that effect, Case C-343/09   
Afton Chemical   
EU:C:2010:419, paragraph 45;   
Volker und Markus Schecke and Eifert  
 EU:C:2010:662, paragraph 74; Cases C-581/10 and C-629/10   
Nelson and Others  
 EU:C:2012:657, paragraph 71; Case C-283/11   
Sky Österreich  
 EU:C:2013:28, paragraph 50; and Case C-101/12   
Schaible  
 EU:C:2013:661, paragraph 29).  
47      With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature’s discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R.,   
S. and Marper v. the United Kingdom   
[GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).  
48      In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature’s discretion is reduced, with the result that review of that discretion should be strict.  
49      As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.   
50      That assessment cannot be called into question by the fact relied upon in particular by Mr Tschohl and Mr Seitlinger and by the Portuguese Government in their written observations submitted to the Court that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General has pointed out in paragraph 137 of his Opinion.   
51      As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.  
52      So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court’s settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12   
IPI  
 EU:C:2013:715, paragraph 39 and the case-law cited).  
53      In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.  
54      Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R.,   
Liberty and Others v. the United Kingdom  
, 1 July 2008, no. 58243/00, § 62 and 63;   
Rotaru v. Romania  
, § 57 to 59, and   
S. and Marper v. the United Kingdom  
, § 99).  
55      The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR,   
S. and Marper v. the United Kingdom  
, § 103, and   
M. K. v. France  
, 18 April 2013, no. 19522/09, § 35).  
56      As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people’s everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.   
57      In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.   
58      Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.   
59      Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.   
60      Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.  
61      Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.  
62      In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.   
63      Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.  
64      Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.  
65      It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.  
66      Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.  
67      Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.  
68      In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10   
Commission   
v   
Austria  
 EU:C:2012:631, paragraph 37).  
69      Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.  
70      In those circumstances, there is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter.  
71      Consequently, the answer to the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12 is that Directive 2006/24 is invalid.   
   
The first question and the second question, parts (a) and (e), and the third question in Case C-293/12 and the second question in Case C-594/12  
72      It follows from what was held in the previous paragraph that there is no need to answer the first question, the second question, parts (a) and (e), and the third question in Case C-293/12 or the second question in Case C-594/12.  
   
Costs  
73      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national courts, the decision on costs is a matter for those courts. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.

ID: 76ab22b1-321e-4e56-a202-8974501552cf

Judgment of 16 Apr 2015, C-446/12 (  
Willems and Others  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legal obligation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
   
JUDGMENT OF THE COURT (Fourth Chamber)  
16 April 2015 (\*)  
(Reference for a preliminary ruling — Area of freedom, security and justice — Biometric passport — Biometric data — Regulation (EC) No 2252/2004 — Article 1(3) — Article 4(3) — Use of data collected for purposes other than the issue of passports and travel documents — Establishment and use of databases containing biometric data — Legal guarantees — Charter of Fundamental Rights of the European Union — Articles 7 and 8 — Directive 95/46/EC — Articles 6 and 7 — Right to privacy — Right to the protection of personal data — Application to identity cards)  
In Joined Cases C-446/12 to C-449/12,  
REQUESTS for a preliminary ruling under Article 267 TFEU from the Raad van State (Netherlands), made by decision of 28 September 2012, received at the Court on 3 October 2012 (C-446/12), 5 October 2012 (C-447/12) and 8 October 2012 (C-448/12 and C-449/12), in the proceedings  
W.P. Willems  
 (C-446/12)  
v  
Burgemeester van Nuth,  
and  
H.J. Kooistra   
(C-447/12)  
v  
Burgemeester van Skarsterlân,  
and  
M. Roest   
(C-448/12)  
v  
Burgemeester van Amsterdam,  
and  
L.J.A. van Luijk   
(C-449/12)  
v  
Burgemeester van Den Haag,  
THE COURT (Fourth Chamber),  
composed of L. Bay Larsen, President of the Chamber, K. Jürimäe, J. Malenovský (Rapporteur), M. Safjan and A. Prechal, Judges,  
Advocate General: P. Mengozzi,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 6 November 2014,  
after considering the observations submitted on behalf of:  
–        Mr Willems, by himself,  
–        Mr Kooistra, by himself,  
–        Ms Roest and Ms van Luijk, by J. Hemelaar, advocaat,  
–        the Netherlands Government, by J. Langer, M. Bulterman and H. Stergiou, acting as Agents,  
–        the French Government, by F.-X. Bréchot, acting as Agent,  
–        the Swiss Government, by D. Klingele, acting as Agent,  
–        the European Parliament, by P. Schonard and R. van de Westelaken, acting as Agents,  
–        the Council of the European Union, by E. Sitbon, I. Gurov and K. Michoel, acting as Agents,  
–        the European Commission, by B. Martenczuk and G. Wils, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern the interpretation of Articles 1(3) and 4(3) of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ 2004 L 385, p. 1), as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009 (OJ 2009 L 142, p. 1, and corrigendum OJ 2009 L 188, p. 127) (‘Regulation No 2252/2004’).  
2        The requests have been made in proceedings between Mr Willems, Mr Kooistra, Ms Roest and Ms van Luijk and the Burgemeester van Nuth, the Burgemeester van Skarsterlân, the Burgemeester van Amsterdam and the Burgemeester van Den Haag, respectively (‘the Burgemeesters’), concerning the refusal by the latter to issue the applicants in the main proceedings with a passport (C-446/12, C-448/12 and C-449/12) and an identity card (C-447/12) unless their biometric data was recorded at the same time.  
   
Legal context  
   
EU law  
3        Under Article 6(1)(b), first sentence, of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), Member States are to provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. In accordance with Article 6(1)(c) thereof that data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.  
4        Article 7(c), (e) and (f) of that directive provides that personal data may be processed only if it is necessary ‘for compliance with a legal obligation to which the controller is subject’ or ‘for the performance of a task carried out in the public interest or ‘in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed’ or ‘for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)’.  
5        According to Article 4(1) of Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ 2009 L 158, p. 77):  
‘Without prejudice to the provisions on travel documents applicable to national border controls, all Union citizens with a valid identity card or passport and their family members who are not nationals of a Member State and who hold a valid passport shall have the right to leave the territory of a Member State to travel to another Member State.’   
6        Article 5(1) of that directive provides:   
‘Without prejudice to the provisions on travel documents applicable to national border controls, Member States shall grant Union citizens leave to enter their territory with a valid identity card or passport and shall grant family members who are not nationals of a Member State leave to enter their territory with a valid passport.’   
7        Under Article 1(2) and (3) of Regulation No 2252/2004:   
‘2. Passports and travel documents shall include a storage medium which shall contain a facial image. Member States shall also include fingerprints in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.  
…  
3. This Regulation applies to passports and travel documents issued by Member States. It does not apply to identity cards issued by Member States to their nationals or to temporary passports and travel documents having a validity of 12 months or less.’  
8        Article 4(3), first subparagraph, of the regulation reads as follows:   
‘Biometric data shall be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. For the purpose of this Regulation the biometric features in passports and travel documents shall only be used for verifying:   
(a)      the authenticity of the passport or travel document;   
(b)      the identity of the holder by means of directly available comparable features when the passport or travel document is required to be produced by law.’  
9        In accordance with Recital 5 in the preamble to Regulation No 444/2005, which amended Regulation No 2252/2004:  
‘Regulation … No 2252/2004 requires biometric data to be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. This is without prejudice to any other use or storage of these data in accordance with national legislation of Member States. Regulation … No 2252/2004 does not provide a legal base for setting up or maintaining databases for storage of those data in Member States, which is strictly a matter of national law.’  
   
Netherlands law  
10      Pursuant to Article 2(1), introductory, part (a), of the Law laying down the rules for the issue of travel documents (Rijkswet houdende het stellen van regelen betreffende de verstrekking van reisdocumenten) of 26 September 1991 (Stb. 1991, No 498, ‘the Passport Law’), the national passport is one of the travel documents issue by the Kingdom of the Netherlands.  
11      According to Article 2(2) thereof, the Netherlands identity card is a travel document relating to the European part of the Kingdom of the Netherlands, valid for countries which are parties to the European Agreement on Regulations governing the Movement of Persons between Member States of the Council of Europe, adopted in Paris on 13 December 1957.   
12      Article 3(3) of that law, in the version in force at the material time, provides that a travel document must contain a facial image, two fingerprints and the signature of the holder. Article 3(8) thereof states that the competent issuing authorities are required to keep records of the travel documents issued.  
13      Article 65(1) and (2) of the Passport Law, in the version in force at the material time, provided:  
‘1.      The authority which issues travel documents shall retain the following data in the records referred to in Article 3(8), second sentence:  
a.      fingerprint data referred to in Article 3(3);   
b.      two other fingerprints, as specified by the competent Minister, of the person applying for a travel document;  
2.      The data referred to in paragraph 1 may be provided solely to authorities, institutions and individuals charged with the implementation of this law, in so far as they require the data for such implementation.  
14      The Passport Law also contains Articles 4a and 4b, but they had not entered into force at the material time, a royal decree being required for that purpose. Article 4a of that law provided that a minister was to keep a central register of travel documents in which the data relating to travel documents are to be stored. That central register was to contain the data referred to in Article 3 of that law and two digital fingerprints from the applicant different than those in the travel document, pursuant to Article 3(3) of that law. Article 4b of the Passport Law set out the conditions under which the data stored in the central register for travel documents could be communicated to other institutions, bodies or persons, in particular, for the purpose of identifying victims of disasters and accidents, the detection and prosecution of criminal offences and for the conduct of investigations of acts constituting a threat to State security.  
15      Articles 3, 4a, 4b and 65 of the Passport Law were amended with effect from 20 January 2014. Pursuant to Article 3(9) of that law, inserted following that legislative amendment, digital fingerprints are to be stored only for the duration of the procedure for application and issue of the passport, that is to say until the passport is issued to the holder. After issue of the new passport, the digital fingerprints are to be erased. Articles 4a and 4b of that law have been amended so that they no longer provide for the central storage and communication to third parties of the digital fingerprints taken. Article 65(1) and (2) of that law was repealed and replaced by Article 3(9).  
   
The actions in the main proceedings and the questions referred for a preliminary ruling  
16      Mr Willems and Ms Roest and Ms van Luijk each made passport applications. In each case, the Burgemeester concerned rejected those applications, since the persons in question had refused to provide digital fingerprints. Mr Kooistra made an application for the issue of a Netherlands identity card which was also refused on the ground that he had refused to provide digital fingerprints and a facial image.  
17      The applicants in the main proceedings refused to provide that biometric data on the ground that creating and storing it constitute a serious breach of their physical integrity and their right to privacy.  
18      According to the applicants in the main proceedings that breach arises, inter alia, from the storage of that data on three different media. The data is stored not only on the storage medium integrated into the Netherlands passport or identity card, but also on a decentralised database. In addition, data security risks will increase because the Passport Law provides that local authority databases are eventually to be combined into in a centralised database.  
19      Furthermore, there are no provisions clearly identifying the persons who will have access to biometric data, so that the applicants in the main proceedings will lose control of that data.  
20      Similarly, the applicants in the main proceedings submit that in the future the authorities might use biometric data for purposes other than those for which it was provided to them. In particular, the storage of that data in a database might lead to its use for judicial purposes or by the intelligence and security services. It follows from Regulation No 2252/2004 that, for the purposes of the application of that regulation, biometric data, such as digital fingerprints, may be used only in order to verify the authenticity of the document and the identity of the holder. Such use is also contrary to fundamental rights.  
21      Since their respective actions against the decisions of the Burgemeesters were rejected at first instance, the applicants in the main proceedings have brought appeals before the referring court.  
22      The referring court asks, first of all, whether, in Case C-447/12, the Netherlands identity card falls within the scope of Regulation No 2252/2004. In that connection, it is clear from EU law on the free movement of persons that an identity card is also a travel document within the European Union. Furthermore, that card enables travel outside the European Union, to EU candidate countries. Moreover, it is conceivable that Article 1(3) thereof may be read as meaning that the concept of ‘identity card’ for the purposes of that provision must be read together with the expression ‘having a validity of 12 months or less’ which also appears in that provision. Netherlands identity cards are valid for five years.  
23      Next, the referring court indicates that the outcome of the cases in the main proceedings will depend on whether the ground relied on by the applicants, according to which the purposes for which the data collected for the issue of a passport or a travel document may be used in the future are unclear, is well founded.   
24      Lastly, that court asks whether it follows from Regulation No 2252/2004 that it must be guaranteed by law, that is to say, by means of a mandatory rule of general scope, that the biometric data collected on the basis of that regulation may not be used for purposes other than those set out therein.  
25      In those circumstances, the Raad van State decided to stay the proceedings and to refer two questions for a preliminary ruling in Cases C-446/12, C-448/12 and C-449/12 and three questions in Case C-447/12.  
26      The first questions in Cases C-446/12, C-448/12 and C-449/12 and the second question in Case C-447/12 concerned the validity of Article 1(2) of Regulation No 2252/2004. They corresponded to the question referred for a preliminary ruling which gave rise to the judgment in   
Schwarz   
(C-291/12, EU:C:2013:670).  
27      Following that judgment, the referring court withdrew the questions mentioned in the preceding paragraph.  
28      However, the Raad van State maintained the first question referred for a preliminary ruling in Case C-447/12 which is worded as follows:  
‘Must Article 1(3) of [Regulation No 2252/2004] be interpreted as meaning that it does not apply to identity cards, such as the Netherlands identity cards, issued by Member States to their nationals, regardless of their period of validity and regardless of the possibilities of using them as travel documents?’  
29      Likewise, the Raad van State maintained the second questions referred in Cases C-446/12, C-448/12 and C-449/12, and the third question in Case C-447/12, which are identical and are worded as follows:  
‘… [M]ust Article 4(3) of Regulation [No 2252/2004], [read] in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union [“the Charter”], Article 8(2) of the European Convention on the Protection of Human Rights and Fundamental Freedoms[, signed at Rome on 4 November 1950,] and Article 7(f) of [Directive 95/46], read in conjunction with Article 6(1)(b) of that directive, be interpreted as meaning that, when the Member States give effect to Regulation No 2252/2004, there should be a statutory guarantee that the biometric data collected and stored pursuant to that regulation may not be collected, processed and used for any purposes other than the issuing of the document concerned?’  
   
Consideration of the questions referred for a preliminary ruling  
   
The first question in Case C-447/12  
30      By its question, the referring court asks essentially if Article 1(3) of Regulation No 2252/2004 must be interpreted as meaning that that regulation is not applicable to identity cards issued by a Member State to its nationals, such as the Netherlands identity cards, irrespective of the period of their validity and irrespective of the possibility to use them for the purposes of travel outside that State.  
31      According to Article 1(3), second sentence, Regulation No 2252/2004 does not apply to identity cards issued by Member States to their nationals or to temporary passports and to travel documents having a validity of 12 months or less.  
32      In the first place, it must be established whether the scope of Regulation No 2252/2004 varies according to the period of validity of an identity card.  
33      In that connection, it is clear from Article 1(3), second sentence, of that regulation that that provision restricts the scope of the regulation by excluding from it two categories of documents. Given that those two categories of documents are connected in the text by the conjunction ‘or’, they must be regarded as being separate from one another.  
34      That conclusion is supported by the fact that in several language versions of Article 1(3), second sentence, of Regulation No 2252/2004, and in particular, in the English (‘temporary passports and travel documents having a validity of 12 months or less’), German (‘vorläufige Pässe und Reisedokumente mit enier Gültigkeitsdauer von zwölf Monaten oder weniger’) and Dutch (‘tijdelijke paspoorten en reisdocumenten die een geldigheidsduur van 12 maanden of minder hebben’) language versions, the expressions ‘temporary’ and ‘having a validity of 12 months or less’ do not apply to one of the categories of documents mentioned in the preceding paragraph, namely identity cards issued by the Member States.  
35      In those circumstances, it must be stated that the expressions ‘temporary’ and ‘having a validity of 12 months or less’ do not concern identity cards issued by the Member States to their nationals.  
36      It follows that, according to the wording of Article 1(3) of Regulation No 2252/2004, that regulation does not apply to identity cards issued by Member States to their nationals, whether or not they are temporary and whatever the period of their validity.  
37      Moreover, that conclusion is reinforced by the   
travaux préparatoires  
 for Regulation No 2252/2004. In particular from Article 1(3) of the Draft Council Regulation on standards for security features and biometrics in travel documents issued by Member States (Council Document No 11489/04 of 26 July 2004) stated that that regulation is intended to apply ‘to passports and travel documents with a validity of 12 months or more. It does not apply to identity cards issued by Member States to their nationals’.  
38      In the second place, it must be established whether the fact that identity cards such as Netherlands identity cards may be used for the purposes of travel within the European Union and to certain non-Member States may bring it within the scope of Regulation No 2252/2004.  
39      In that connection, it must be observed that it is true that identity cards, such as Netherlands identity cards, may serve as identification of the holder with regard to non-Member States which have concluded bilateral agreements with the Member State concerned, and, in accordance with Articles 4 and 5 of Directive 2004/38, for the purposes of travel between several Member States.  
40      However, it is clear from the wording of the second sentence of Article 1(3) of Regulation No 2252/2004, interpreted in the light of the findings in paragraphs 32 to 37 of the present judgment, that the EU legislature expressly decided to exclude from the scope of that regulation identity cards issued by Member States to their nationals.  
41      Consequently, the fact that identity cards, such as Netherlands identity cards, may be used for the purposes of travel within the European Union and to a limited number of non-Member States, does not bring them within the scope of Regulation No 2252/2004.  
42      Having regard to the foregoing considerations, the answer to the question referred is that Article 1(3) of Regulation No 2252/2004 must be interpreted as meaning that that regulation is not applicable to identity cards issued by a Member States to its nationals, such as Netherlands identity cards, regardless of the period of validity and the possibility of using them for the purposes of travel outside that State.  
   
The second questions in Cases C-446/12, C-448/12 and C-449/12, and the third question in Case C-447/12  
43      By those questions, which it is appropriate to examine together, the referring court asks essentially whether Article 4(3) of Regulation No 2252/2004, read together with Articles 6 and 7 of Directive 95/46 and Articles 7 and 8 of the Charter, must be interpreted as meaning that it requires Member States to guarantee that the biometric data collected and stored pursuant to that regulation will not be collected, processed and used for purposes other than the issue of passports or other travel documents.  
44      In that connection, it must be observed at the outset that, having regard to the answer to the first question in Case C-447/12, it is only necessary to examine the questions raised in relation to Cases C-446/12, C-448/12 and C-449/12.  
45      Article 4(3) of Regulation No 2252/2004 requires that, in order to issue a passport or travel document, biometric data must be ‘collected’ and ‘stored’ on the storage medium integrated into those documents. As regards the ‘use’ of that data, that provision states that, for the purposes of that regulation, the latter are to be used only for verifying the authenticity of the document or the identity of the holder when the passport or other travel documents are required to be produced by law.  
46      The Court has already held, in its judgment in   
Schwarz   
(C-291/12, EU:C:2013:670), that the use and storage of biometric data for the purposes specified in Article 4(3) of that regulation are compatible with the requirements of Articles 7 and 8 of the Charter.  
47      As regards all other uses and storage of that data, it is clear from Article 4(3) of Regulation No 2252/2004, which deals with the use of such data ‘[f]or the purpose of this Regulation’, read in the light of recital 5 in the preamble to Regulation No 444/2009, which amended Regulation No 2252/2004, that the use and storage of that data are not governed by the latter regulation. That recital states that Regulation No 2252/2004 is without prejudice to any other use or storage of these data in accordance with national legislation of Member States and that it does not provide a legal base for setting up or maintaining databases for storage of those data in Member States, that matter being within the exclusive competence of the Member States.  
48      It follows, in particular, that Regulation No 2252/2004 does not require a Member State to guarantee in its legislation that biometric data will not be used or stored by that State for purposes other than those mentioned in Article 4(3) of that regulation (see, to that effect, judgment in   
Schwarz  
, C-291/12, EU:C:2013:670, paragraph 61).  
49      Next, as regards Articles 7 and 8 of the Charter, it is clear from the case-law of the Court that the fundamental rights guaranteed by the Charter must be respected where national legislation falls within the scope of EU law. In other words, the applicability of EU law entails the applicability of the fundamental rights guaranteed by the Charter (judgments in   
Åkerberg Fransson  
, C-617/10, EU:C:2013:105, paragraphs 20 and 22, and   
Texdata Software  
, C-418/11, EU:C:2013:588, paragraphs 71 to 73).  
50      Given that, in the present case, Regulation No 2252/2004 is not applicable, there is no need to determine whether the storage and use of biometric data for purposes other than those referred to in Article 4(3) thereof are compatible with those articles of the Charter.  
51      The foregoing considerations are without prejudice to any examination by the national courts of the compatibility of all the national measures relating to the use and storage of biometric data with their national law and, if appropriate, with the European Convention on the Protection of Human Rights and Fundamental Freedoms (see, to that effect, judgment in   
Schwarz  
, C-291/12, EU:C:2013:670, paragraph 62).  
52      Finally, as regards Articles 6 and 7 of Directive 95/46, it must be observed that, by its questions, the referring court requests the interpretation of Regulation No 2252/2004 and only that regulation. Since it follows from the foregoing considerations that that regulation is not applicable in the present case, there is no need to examine, as a separate matter, whether those articles affect the national legal framework relating to the storage and use of biometric data outside the scope of Regulation No 2252/2004.   
53      Therefore, the answer to the questions referred is that Article 4(3) of Regulation No 2252/2004 must be interpreted as meaning that it does not require the Member States to guarantee, in their legislation, that biometric data collected and stored in accordance with that regulation will not be collected, processed and used for purposes other than the issue of the passport or travel document, since that is not a matter which falls within the scope of that regulation.  
   
Costs  
54      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.   
On those grounds, the Court (Fourth Chamber) hereby rules:  
1.        
Article 1(3) of of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009, must be interpreted as meaning that that regulation is not applicable to identity cards issued by a Member States to its nationals, such as Netherlands identity cards, regardless of the period of validity and the possibility of using them for the purposes of travel outside that State.  
2.        
Article 4(3) of Regulation No 2252/2004, as amended by Regulation No 444/2009, must be interpreted as meaning that it does not require the Member States to guarantee, in their legislation, that biometric data collected and stored in accordance with that regulation will not be collected, processed and used for purposes other than the issue of the passport or travel document, since that is not a matter which falls within the scope of that regulation.

ID: 78d50b52-8a8e-4dde-8f0a-e31a162cce98

of 11 Nov 2020, C-61/19 (  
Orange Romania  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Consent   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Information to be provided in case of direct collection   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness, fairness and transparency   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accountability   
   
JUDGMENT OF THE COURT (Second Chamber)  
11 November 2020 (\*)  
(Reference for a preliminary ruling – Directive 95/46/EC – Article 2(h) and Article 7(a) – Regulation (EU) 2016/679 – Article 4(11) and Article 6(1)(a) – Processing of personal data and protection of private life Collection and storage of the copies of identity documents by a provider of mobile telecommunications services Concept of the data subject’s ‘consent’ – Freely given, specific and informed indication of wishes – Declaration of consent by means of a tick box Signing of the contract by the data subject – Burden of proof)  
In Case C-61/19,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Tribunalul Bucureşti (Regional Court of Bucharest, Romania), made by decision of 14 November 2018, received at the Court on 29 January 2019, in the proceedings  
Orange România SA  
v  
Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP),  
THE COURT (Second Chamber),  
composed of A. Arabadjiev, President of the Chamber, T. von Danwitz (Rapporteur) and P.G. Xuereb, Judges,  
Advocate General: M. Szpunar,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 11 December 2019,  
after considering the observations submitted on behalf of:  
–        Orange România SA, by D.-D. Dascălu, A.-M. Iordache, and I. Buga , avocaţi,  
–        the Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), by A.G. Opre and I. Ilie, acting as Agents,  
–        the Romanian Government, initially by E. Gane, O.-C. Ichim, L. Liţu and C.-R. Canţăr, and subsequently by E. Gane, O.-C. Ichim and L. Liţu, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by M. Russo, avvocato dello Stato,  
–        the Austrian Government, initially by J. Schmoll and G. Hesse, and subsequently by J. Schmoll, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes, P. Barros da Costa, L. Medeiros and I. Oliveira, acting as Agents,  
–        the European Commission, by H. Kranenborg, D. Nardi and L. Nicolae, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 4 March 2020,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2(h) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) and of Article 4(11) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).  
2        The request has been made in proceedings between Orange România SA and the Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (the National Authority for the Supervision of Personal Data Processing, Romania), concerning an action for annulment of a decision by which the ANSPDCP imposed a fine on Orange România for collecting and storing copies of customers’ identity documents without their valid consent and ordered it to destroy those copies.  
   
Legal context  
   
EU law  
   
Directive 95/46  
3        Recital 38 of Directive 95/46 provides that, ‘if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection’.  
4        Article 2(h) of that directive provides that, for the purposes of the directive:   
‘“the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.’  
5        Article 6 of that directive states:  
‘1.      Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;   
…  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
6        As set out in Article 7(a) of Directive 95/46:  
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent …’  
7        Article 10 of that directive reads as follows:  
‘Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:  
(a)      the identity of the controller and of his representative, if any;  
(b)      the purposes of the processing for which the data are intended;  
(c)      any further information such as  
–        the recipients or categories of recipients of the data,  
–        whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,  
–        the existence of the right of access to and the right to rectify the data concerning him   
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.’  
   
Regulation 2016/679  
8        Recitals 32 and 42 of Regulation 2016/679 state:   
‘(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.  
…  
(42) Where processing is based on the data subject’s consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC [of 5 April 1993 on unfair terms in consumer contracts, (OJ 1993 L 95, p. 29)], a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.’  
9        Article 4(11) of that regulation provides:  
‘“consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.’  
10      Article 5 of that regulation provides:   
‘1.      Personal data shall be:   
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);   
…  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
11      In accordance with Article 6(1)(a) of Regulation 2016/679:  
‘1. Processing shall be lawful only if and to the extent that at least one of the following applies:   
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;   
…’  
12      Article 7(1),(2) and (4) of Regulation 2016/679 is worded as follows:  
‘1.      Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.  
2.      If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.  
…  
4.      When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.’  
13      Article 13(1) and (2) states:  
‘1.      Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:   
(a)      the identity and the contact details of the controller and, where applicable, of the controller’s representative;  
…  
(c)      the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;   
…  
2.      In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:  
(a)      the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;  
(b)      the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;  
(c)      where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal’.  
14      Article 94(1) of Regulation 2016/679 provides:  
‘Directive 95/46/EC is repealed with effect from 25 May 2018.’  
15      Article 99(2) of Regulation 2016/679 provides that that regulation is to apply from 25 May 2018.  
   
Romanian law  
16      The legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Law No 677/2001 on the protection of persons with regard to the processing of personal data and on the free movement of such data) (  
Monitorul Oficial al României,  
 Part I, No 790 of 12 December 2001) is intended to transpose the provisions of Directive 95/46 into national law.  
17      Article 5(1) of that law provides:  
‘(1)      Any processing of personal data, except for the processing which refers to the categories mentioned in Article 7(1) and Articles 8 and 10, may be carried out only if the data subject has given his or her express and unambiguous consent for that processing.  
…’  
18      In accordance with Article 8 of that law:   
‘(1)      The processing of an individual’s personal identification number or of other personal data having a generally applicable identification purpose may be carried out only if:  
(a)      the data subject has expressly given his or her consent, or  
(b)      the processing is expressly provided for by a provision of law.  
(2)      The supervisory authority may also establish other cases in which the processing of the data referred to in paragraph 1 may be carried out, provided that adequate safeguards are in place to protect the rights of data subjects.’  
19      Article 32 of Law 677/2001 is worded as follows:  
‘The processing of personal data by a controller, or by a person mandated by him or her, in breach of Articles 4 to 10 or without due regard to the rights provided for in Articles 12 to 15 or in Article 17, shall constitute an administrative offence, unless it is carried out in such circumstances as to constitute a criminal offence, and shall be penalised by a fine of between RON [1 000] and RON [25 000].’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
20      Orange România is a provider of mobile telecommunications services on the Romanian market.  
21      By decision of 28 March 2018, the ANSPDCP imposed a fine on Orange România for storing copies of customers’ identity documents without demonstrating that those customers had given their valid consent, and also required it to destroy those copies.  
22      In that decision, the ANSPDCP stated that between 1 and 26 March 2018, Orange România had concluded contracts in writing for the provision of mobile telecommunications services with individuals and that copies of those persons’ identity documents were annexed to those contracts. According to the ANSPDCP, Orange România has not proven that the customers whose identity documents had been copied and annexed to their contracts had given their valid consent to the collection and storage of copies of their identity documents.  
23      The relevant clauses of the contracts in question read as follows:  
‘–      The customer states that:  
(i)      he or she has been informed, prior to concluding the contract, of the chosen tariff plan, the applicable tariffs, the minimum duration of the contract, the conditions for its termination, the conditions for accessing and using the services, including service coverage areas, …;  
(ii)      Orange România has provided the customer with all the necessary information to enable him or her to give his or her unvitiated, express, free and specific consent to the conclusion and express acceptance of the contract, including all the contractual documentation, the General Terms and Conditions for using Orange’s services and the Brochure of Tariffs and Services;  
(iii)      he or she has been informed of, and has consented to, the following:  
–        the processing of personal data for the purposes referred to in Article 1.15 of the General Terms and Conditions for using Orange’s services;  
–        the storage of copies of documents containing personal data for identification purposes;  
–        the agreement for the processing of personal data (contact number and email address) for direct marketing purposes;  
–        the agreement for the processing of personal data (contact number and email address) for market research purposes;  
–        I have read and expressly agree to the storage of copies of documents containing personal data relating to state of health;  
–        the data referred to in Article 1.15(10) of the General Terms and Conditions for Orange’s services are not included in subscriber information and subscriber directory services.’  
24      Orange România brought an action against the decision of 28 March 2018 before the Tribunalul Bucureşti (Regional Court, Bucharest, Romania).  
25      According to the findings of the referring court, there are both contracts in which a cross has been placed in the box for the clause relating to the storage of copies of documents with personal data for identification purposes and also contracts in which there is no such cross. That court explains that, notwithstanding the stipulations of its General Terms and Conditions, Orange România did not refuse to conclude subscription contracts with customers who refused to consent to the storage of a copy of one of their identity documents. That court also notes that Orange România’s ‘internal procedures’ relating to sales stated that that refusal had to be set out in a specific form, to be signed by those customers before concluding the contract.  
26      The referring court raises the question whether, in those circumstances, the customers concerned may be regarded as having validly consented to the collection of their identity document and to copies of that document being annexed to the contracts. Furthermore, that court is uncertain whether the signing of a contract with a clause on the storage of copies of documents containing personal data for identification purposes can prove the existence of such consent.  
27      In those circumstances the Tribunalul București (Regional Court, Bucharest) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      For the purposes of Article [2](h) of Directive 95/46, what conditions must be fulfilled in order for an indication of wishes to be regarded as specific and informed?  
(2)      For the purposes of Article 2(h) of Directive 95/46, what conditions must be fulfilled in order for an indication of wishes to be regarded as freely given?’  
   
Consideration of the questions referred  
28      As a preliminary matter, it is appropriate to determine the applicability of Directive 95/46 and Regulation 2016/679 to the facts at issue in the main proceedings.  
29      Directive 95/46 was repealed with effect from 25 May 2018 and replaced by Regulation 2016/679, in accordance with Article 94(1) and Article 99(2) of that regulation.  
30      Accordingly, as the decision of the ANSPDCP at issue in the main proceedings was adopted on 28 March 2018 and, therefore, before 25 May 2018, the referring court is fully entitled to find that Directive 95/46 applies   
ratione temporis  
 to the main proceedings.  
31      That being so, it is also apparent from the file before the Court that, by its decision, the ANSPDCP not only imposed a fine on Orange România, but also ordered it to destroy the copies of the identity documents at issue, and that the main proceedings also concern that latter order. As nothing in that file shows that that order was complied with before 25 May 2018, it is not inconceivable that, in the present case, Regulation 2016/679 is applicable   
ratione temporis  
 to that order (see, to that effect, judgment of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraph 41).  
32      In those circumstances, in order to enable the Court to provide useful answers to the questions submitted by the referring court, those questions must be answered on the basis of both Directive 95/46 and Regulation 2016/679 (see, by analogy, judgment of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraph 43).  
33      By its two questions referred for a preliminary ruling, which should be examined together, the referring court asks, in essence, whether Article 2(h) and Article 7(a) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679 must be interpreted as meaning that a contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is capable of demonstrating that that person’s consent has been validly given, as provided for in those provisions, to that collection and storage.  
34      In that regard, it should be borne in mind that Article 7 of Directive 95/46 and Article 6 of Regulation 2016/679 set out an exhaustive list of the cases in which the processing of personal data can be regarded as being lawful (see, regarding Article 7 of Directive 95/46, judgments of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 57 and the case-law cited, and of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraph 53). In particular, Article 7(a) of that directive and Article 6(1)(a) of that regulation provide that the data subject’s consent may make such processing lawful.  
35      As regards the requirements to which such consent is subject, Article 7(a) of Directive 95/46 provides that the data subject must have ‘unambiguously given his consent’, while Article 2(h) of that directive defines the term ‘consent’ as meaning ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’. To the extent that those provisions set out that the data subject is to give an ‘indication of his wishes’ in order to give ‘unambiguously’ his consent, only active behaviour by that person with a view to giving his or her consent may be relevant (see, to that effect, judgment of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraphs 52 and 54).  
36      That same requirement also operates in the context of Regulation 2016/679. Indeed, the wording of Article 4(11) of that regulation, which defines the ‘consent of the data subject’ for the purposes, inter alia, of Article 6(1)(a) of that regulation, appears even more stringent than Article 2(h) of Directive 95/46, in that it requires a ‘freely given, specific, informed and unambiguous’ indication of the data subject’s wishes in the form of a statement or by ‘a clear affirmative action’ signifying agreement to the processing of personal data relating to him or her. Accordingly, active consent is now expressly laid down in Regulation 2016/679 (see, to that effect, judgment of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraphs 61 to 63).  
37      In that regard, while recital 32 of that regulation states that consent could be given, inter alia, by ticking a box when visiting an internet website, on the contrary, it expressly excludes the possibility that ‘silence, pre-ticked boxes or inactivity’ constitute consent. As the Court has held, in such a situation, it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not deselecting a checkbox pre-ticked beforehand nor, in any event, whether that consent had been informed. It is not inconceivable that a user would not have read the information accompanying the preselected checkbox, or even would not have noticed that checkbox, before continuing with his or her activity on the website visited (see, to that effect, judgment of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraphs 55 and 57).  
38      Furthermore, Article 2(h) of Directive 95/46 and Article 4(11) of Regulation 2016/679 require a ‘specific’ indication of the data subject’s wishes in the sense that it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject’s wishes for other purposes (see, regarding Article 2(h) of Directive 95/46, judgment of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraph 58).  
39      In that regard, the first sentence of Article 7(2) of that regulation states that if the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent is to be presented in a manner which is clearly distinguishable from the other matters. In particular, it is apparent from that provision, read in conjunction with recital 42 of that regulation, that such a declaration must be presented in an intelligible and easily accessible form, using clear and plain language, in particular where it concerns a declaration of consent which is to be pre-formulated by the controller of personal data.  
40      As regards the requirement arising from Article 2(h) of Directive 95/46 and Article 4(11) of Regulation 2016/679 that consent must be ‘informed’, that requirement implies, in accordance with Article 10 of that directive, read in the light of recital 38 thereof, and with Article 13 of that regulation, read in the light of recital 42 thereof, that the controller is to provide the data subject with information relating to all the circumstances surrounding the data processing, in an intelligible and easily accessible form, using clear and plain language, allowing the data subject to be aware of, inter alia, the type of data to be processed, the identity of the controller, the period and procedures for that processing and the purposes of the processing. Such information must enable the data subject to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed (see, by analogy, judgment of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraph 74).  
41      Furthermore, as the Commission noted in its observations submitted to the Court, it is clear from the second indent of Article 10(c) of Directive 95/46 and from Article 13(2)(b) and (c) of Regulation 2016/679, read in the light of recital 42 of that regulation, that, in order to ensure that the data subject enjoys genuine freedom of choice, the contractual terms must not mislead him or her as to the possibility of concluding the contract even if he or she refuses to consent to the processing of his or her data. Without information of that kind, the data subject’s consent to the processing of his or her personal data cannot be regarded as having been given freely or, moreover, as having been given in an informed manner.  
42      It is appropriate to add that under Article 6(1)(a) and (2) of Directive 95/46 and Article 5(1)(a) of Regulation 2016/679, the controller of personal data is required to ensure, inter alia, the lawfulness of the processing of those data and, as stated in Article 5(2) of that regulation, must be able to demonstrate that lawfulness. As regards, more specifically, the data subject’s possible consent, Article 7(a) of that directive provides that the data subject must have ‘unambiguously’ given his or her consent, which implies, as the Advocate General stated in point 56 of his Opinion, that the controller bears the burden of proof relating to the existence of valid consent. Article 7(1) of that regulation now provides that where processing is based on consent, that controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data.  
43      In the present case, Orange România stated, in its observations to the Court, that, during the procedure for concluding the contracts at issue in the main proceedings, its sales agents informed the customers concerned, before concluding the contracts, inter alia, of the purposes of collecting and storing copies of the identity documents and of their choice as to that collection and storage, before obtaining their oral consent to that collection and storage. According to Orange România, the box relating to the storage of copies of identity documents was therefore ticked solely on the basis of the individuals’ freely expressed agreement to that effect when the contract was concluded.  
44      In those circumstances, the request for a preliminary ruling essentially seeks to clarify whether the consent thus invoked as regards such processing of personal data may be established on the basis of the contractual clauses in those contracts.  
45      In that regard, it is apparent from the information set out in that request that, although those contracts contain a clause stating that the customers concerned have been informed of, and have given their consent to, the storage of a copy of their identity document for identification purposes, the box relating to that clause had already been ticked by Orange România’s sales agents before those customers signed in acceptance of all the clauses, that is to say, both of that clause and of clauses not linked to data protection. The request further states that although not specified in the contracts at issue in the main proceedings, Orange România agreed to conclude those contracts with customers who refused to consent to a copy of their identity document being stored, and at the same time required in that case that those customers sign a specific form setting out their refusal.  
46      Since, according to the information in the request for a preliminary ruling, the customers concerned do not appear to have themselves ticked the box relating to that clause, the mere fact that that box was ticked is not such as to establish a positive indication of those customers’ consent to a copy of their identity card being collected and stored. As the Advocate General observed in point 45 of his Opinion, the fact that those customers signed the contracts containing the ticked box does not, on its own, prove such consent, in the absence of any indications confirming that that clause was actually read and digested. It is for the referring court to carry out the necessary investigations to that end.  
47      Furthermore, to the extent that the ticked clause relating to the processing of those data does not appear to have been presented in a form which clearly distinguishes it from the other contractual clauses, it is for that court to assess, in the light of the considerations in paragraph 34 above, whether the signature to those contracts relating to a number of contractual clauses may be regarded as indicating specific consent to the collection and storage of personal data, within the meaning of Article 2(h) of Directive 95/46 and Article 4(11) of Regulation 2016/679.  
48      Moreover, since the contractual clause at issue in the main proceedings merely states, without giving any further details, that storage of the copies of the identity cards is for identification purposes, it is for the referring court to ascertain whether the information provided to the data subjects satisfies the requirements of Article 10 of Directive 95/46 and Article 13 of Regulation 2016/679, which set out the information which the controller must provide to a data subject when collecting data which concern that person in order to ensure fair processing of data with regard to him or her.  
49      It is also for the referring court to assess, in particular, whether the contractual terms at issue in the main proceedings were capable of misleading the data subject as to the possibility of concluding the contract notwithstanding a refusal to consent to the processing of his or her data, in the absence of specific details on that point, thereby calling into question the informed nature of the consent expressed by the signature.  
50      Furthermore, as the Advocate General observed in point 60 of his Opinion, the free nature of that consent appears to be called into question by the fact that, if that consent is refused, Orange România, departing from the normal procedure for concluding the contract, required the customer concerned to declare in writing that he or she did not consent to a copy of his or her identity document being collected or stored. As the Commission observed at the hearing, such an additional requirement is liable to affect unduly the freedom to choose to object to that collection and storage, which it is also for the referring court to determine.  
51      In any event, as is apparent from the considerations set out in paragraphs 35, 36 and 42 above, it is for Orange România, as the data controller, to establish that its customers have, by active behaviour, given their consent to the processing of their personal data, with the result that that company cannot require them actively to express their refusal.  
52      In the light of the foregoing considerations, the answer to the questions referred is that Article 2(h) and Article 7(a) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679 must be interpreted as meaning that it is for the data controller to demonstrate that the data subject has, by active behaviour, given his or her consent to the processing of his or her personal data and that he or she has obtained, beforehand, information relating to all the circumstances surrounding that processing, in an intelligible and easily accessible form, using clear and plain language, allowing that person easily to understand the consequences of that consent, so that it is given with full knowledge of the facts. A contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent, as provided for in those provisions, to that collection and storage, where   
–        the box referring to that clause has been ticked by the data controller before the contract was signed, or where  
–        the terms of that contract are capable of misleading the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or where   
–        the freedom to choose to object to that collection and storage is unduly affected by that controller in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal.  
   
Costs  
53      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
Article 2(h) and Article 7(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Article 4(11) and Article 6(1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that it is for the data controller to demonstrate that the data subject has, by active behaviour, given his or her consent to the processing of his or her personal data and that he or she has obtained, beforehand, information relating to all the circumstances surrounding that processing, in an intelligible and easily accessible form, using clear and plain language, allowing that person easily to understand the consequences of that consent, so that it is given with full knowledge of the facts. A contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent, as provided for in those provisions, to that collection and storage, where  
–          
the box referring to that clause has been ticked by the data controller before the contract was signed, or where  
–          
the terms of that contract are capable of misleading the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or where   
–          
the freedom to choose to object to that collection and storage is unduly affected by that controller, in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal.

ID: 7c56ebad-7863-4dc0-8d5f-14c385d8b01a

Judgment of 29 Jul 2019, C-40/17 (  
Fashion ID  
)  
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Representation of data subjects   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Joint controllers   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Consent   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Transparent information, communication and modalities for the exercise of the rights of the data subject   
   
JUDGMENT OF THE COURT (Second Chamber)  
29 July 2019 (\*)  
(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Article 2(d) — Notion of ‘controller’ — Operator of a website who has embedded on that website a social plugin that allows the personal data of a visitor to that website to be transferred to the provider of that plugin — Article 7(f) — Lawfulness of data processing — Taking into account of the interest of the operator of the website or of that of the provider of the social plugin — Article 2(h) and Article 7(a) — Consent of the data subject — Article 10 — Informing the data subject — National legislation allowing consumer-protection associations to bring or defend legal proceedings)  
In Case C-40/17,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany), made by decision of 19 January 2017, received at the Court on 26 January 2017, in the proceedings  
Fashion ID GmbH & Co. KG  
v  
Verbraucherzentrale NRW eV,  
interveners:  
Facebook Ireland Ltd,  
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen,  
THE COURT (Second Chamber),  
composed of K. Lenaerts, President of the Court, acting as President of the Second Chamber, A. Prechal, C. Toader, A. Rosas (Rapporteur) and M. Ilešič, Judges,  
Advocate General: M. Bobek,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 6 September 2018,  
after considering the observations submitted on behalf of:  
–        Fashion ID GmbH & Co. KG, by C.-M. Althaus and J. Nebel, Rechtsanwälte,  
–        Verbraucherzentrale NRW eV, by K. Kruse, C. Rempe and S. Meyer, Rechtsanwälte,  
–        Facebook Ireland Ltd, by H.-G. Kamann, C. Schwedler and M. Braun, Rechtsanwälte, and by I. Perego, avvocatessa,  
–        Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, by U. Merger, acting as Agent,  
–        the German Government, initially by T. Henze and J. Möller, and subsequently by J. Möller, acting as Agents,  
–        the Belgian Government, by P. Cottin and L. Van den Broeck, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,  
–        the Austrian Government, initially by C. Pesendorfer, and subsequently by G. Kunnert, acting as Agents,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the European Commission, by H. Krämer and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 19 December 2018,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Articles 2, 7, 10 and 22 to 24 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Fashion ID GmbH & Co. KG and Verbraucherzentrale NRW eV concerning Fashion ID’s embedding of a social plugin provided by Facebook Ireland Ltd on the website of Fashion ID.  
   
Legal context  
   
European Union law  
3        With effect from 25 May 2018, Directive 95/46 was repealed and replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1). However, in the light of the date of the facts in the dispute in the main proceedings, it is Directive 95/46 that is applicable to that dispute.  
4        Recital 10 of Directive 95/46 states:  
‘Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of [EU] law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the [European Union]’.  
5        Article 1 of Directive 95/46 provides:  
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
6        Article 2 of that directive provides:  
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or [EU] laws or regulations, the controller or the specific criteria for his nomination may be designated by national or [EU] law;  
…  
(f)      “third party” shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;  
(g)      “recipient” shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;  
(h)      “the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.’  
7        Article 7 of that directive states:  
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent; or  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
8        Article 10 of Directive 95/46, headed ‘Information in cases of collection of data from the data subject’, provides:  
‘Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:  
(a)      the identity of the controller and of his representative, if any;  
(b)      the purposes of the processing for which the data are intended;  
(c)      any further information such as  
–        the recipients or categories of recipients of the data,  
–        whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,  
–        the existence of the right of access to and the right to rectify the data concerning him  
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.’  
9        Article 22 of Directive 95/46 is worded as follows:  
‘Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.’  
10      Article 23 of that directive states:  
‘1.      Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.  
2.      The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.’  
11      Article 24 of that directive provides:  
‘The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.’  
12      Article 28 of Directive 95/46 states:  
‘1.      Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.  
These authorities shall act with complete independence in exercising the functions entrusted to them.  
…  
3.      Each authority shall in particular be endowed with:  
…  
–        the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.  
…  
4.      Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.  
…’  
13      Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11), (‘Directive 2002/58’) provides:  
‘Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
14      Article 1(1) of Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers’ interests (OJ 2009 L 110, p. 30), as amended by Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 (OJ 2013 L 165, p. 1), (‘Directive 2009/22’) provides:  
‘The purpose of this Directive is to approximate the laws, regulations and administrative provisions of the Member States relating to actions for an injunction referred to in Article 2 aimed at the protection of the collective interests of consumers included in the Union acts listed in Annex I, with a view to ensuring the smooth functioning of the internal market.’  
15      Article 2 of that directive provides:  
‘1.      Member States shall designate the courts or administrative authorities competent to rule on proceedings commenced by qualified entities within the meaning of Article 3 seeking:  
(a)      an order with all due expediency, where appropriate by way of summary procedure, requiring the cessation or prohibition of any infringement;  
…’  
16      Article 7 of that directive states:  
‘This Directive shall not prevent Member States from adopting or maintaining in force provisions designed to grant qualified entities and any other person concerned more extensive rights to bring action at national level.’  
17      Article 80 of Regulation 2016/679 reads as follows:  
‘1.      The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects’ rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.  
2.      Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject’s mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.’  
   
German law  
18      Paragraph 3(1) of the version of the Gesetz gegen den unlauteren Wettbewerb (Law against unfair competition) applicable to the dispute in the main proceedings (‘the UWG’) provides:  
‘Unfair commercial practices shall be prohibited.’  
19      Paragraph 3a of the UWG is worded as follows:  
‘A person shall be regarded as acting unfairly where he infringes a statutory provision that is also intended to regulate market behaviour in the interests of market participants and the infringement is liable to have a significantly adverse effect on the interests of consumers, other market participants or competitors.’  
20      Paragraph 8 of the UWG provides:  
‘(1)      Any commercial practice which is unlawful under Paragraph 3 or Paragraph 7 may give rise to an order to cease and desist and, where there is a risk of recurrence, to a prohibition order. An application for a prohibition order may be made as from the time at which there is a risk of such unlawful practice within the meaning of Paragraph 3 or Paragraph 7 occurring.  
…  
(3)      Applications for the orders referred to in subparagraph (1) may be lodged by:  
…  
3.      qualified entities which prove that they are registered on the list of qualified entities pursuant to Paragraph 4 of the Unterlassungsklagegesetz [(Law on injunctions)] or on the list of the European Commission pursuant to Article 4(3) of Directive [2009/22];  
…’  
21      Paragraph 2 of the Law on injunctions provides:  
‘(1)      Any person who infringes the provisions in place to protect consumers (consumer-protection laws), other than in the application or recommendation of general conditions of sale, may have an order to cease and desist and a prohibition order imposed on him in the interests of consumer protection. …  
(2)      For the purposes of this provision, “consumer-protection laws” shall mean, in particular:  
…  
11.      the provisions that regulate the lawfulness   
(a)      of the collection of a consumer’s personal data by a trader, or  
(b)      of the processing or use of personal data collected about a consumer by a trader  
if the data are collected, processed or used for the purposes of publicity, market and opinion research, operation of a credit agency, preparation of personality and usage profiles, address trading, other data trading or comparable commercial purposes.’  
22      Paragraph 12(1) of the Telemediengesetz (Law on telemedia) (‘the TMG’) is worded as follows:  
‘A service provider may collect and use personal data to make telemedia available only in so far as this Law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.’  
23      Paragraph 13(1) of the TMG states:  
‘At the beginning of the use operation the service provider shall inform the user, in a generally understandable way, regarding the nature, extent and purpose of the collection and use of personal data and the processing of his data in States outside the scope of application of Directive [95/46] unless the user has already been informed thereof. In the case of an automated process allowing subsequent identification of the user and which prepares the collection or use of personal data, the user shall be informed at the beginning of this process. The content of the information conveyed to the user must be retrievable for the user at any time.’  
24      Paragraph 15(1) of the TMG provides:  
‘A service provider may collect and use the personal data of a user only to the extent necessary in order to facilitate, and charge for, the use of telemedia (data concerning use). Data concerning use include, in particular:  
1.      features allowing identification of the user,  
2.      information about the beginning, end and extent of the particular use, and  
3.      information about the telemedia used by the user.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
25      Fashion ID, an online clothing retailer, embedded on its website the ‘Like’ social plugin from the social network Facebook (‘the Facebook “Like” button’).  
26      It is apparent from the order for reference that one feature of the internet is that, when a website is visited, the browser allows content from different sources to be displayed. Thus, for example, photos, videos, news and the Facebook ‘Like’ button at issue in the present case can be linked to a website and appear there. If a website operator intends to embed such third-party content, he places a link to the external content on that website. When the browser of a visitor to that website encounters such a link, it requests the content from the third-party provider and adds it to the appearance of the website at the desired place. For this to occur, the browser transmits to the server of the third-party provider the IP address of that visitor’s computer, as well as the browser’s technical data, so that the server can establish the format in which the content is to be delivered to that address. In addition, the browser transmits information relating to the desired content. The operator of a website embedding third-party content onto that website cannot control what data the browser transmits or what the third-party provider does with those data, in particular whether it decides to save and use them.  
27      With regard, in particular, to the Facebook ‘Like’ button, it seems to be apparent from the order for reference that, when a visitor consults the website of Fashion ID, that visitor’s personal data are transmitted to Facebook Ireland as a result of that website including that button. It seems that that transmission occurs without that visitor being aware of it regardless of whether or not he or she is a member of the social network Facebook or has clicked on the Facebook ‘Like’ button.  
28      Verbraucherzentrale NRW, a public-service association tasked with safeguarding the interests of consumers, criticises Fashion ID for transmitting to Facebook Ireland personal data belonging to visitors to its website, first, without their consent and, second, in breach of the duties to inform set out in the provisions relating to the protection of personal data.  
29      Verbraucherzentrale NRW brought legal proceedings for an injunction before the Landgericht Düsseldorf (Regional Court, Düsseldorf, Germany) against Fashion ID to force it to stop that practice.  
30      By decision of 9 March 2016, the Landgericht Düsseldorf (Regional Court, Düsseldorf) upheld in part the requests made by Verbraucherzentrale NRW, after having found that it has standing to bring proceedings under Paragraph 8(3)(3) of the UWG.  
31      Fashion ID brought an appeal against that decision before the referring court, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany). Facebook Ireland intervened in that appeal in support of Fashion ID. Verbraucherzentrale NRW brought a cross-appeal seeking an extension of the ruling made against Fashion ID at first instance.  
32      Fashion ID argues before the referring court that the decision of the Landgericht Düsseldorf (Regional Court, Düsseldorf) is incompatible with Directive 95/46.  
33      First, Fashion ID claims that Articles 22 to 24 of that directive envisage granting legal remedies only to data subjects whose personal data are processed and the competent supervising authorities. Consequently, it argues, the action brought by Verbraucherzentrale NRW is inadmissible due to the fact that that association does not have standing to bring or defend legal proceedings under Directive 95/46.  
34      Second, Fashion ID asserts that the Landgericht Düsseldorf (Regional Court, Düsseldorf) erred in finding that it was a controller, within the meaning of Article 2(d) of Directive 95/46, since it has no influence either over the data transmitted by the visitor’s browser from its website or over whether and, where applicable, how Facebook Ireland uses those data.  
35      In the first place, the referring court has doubts whether Directive 95/46 gives public-service associations the right to bring or defend legal proceedings in order to defend the interests of persons who have suffered harm. It takes the view that Article 24 of that directive does not preclude associations from being a party to legal proceedings, since, pursuant to that article, Member States are required to adopt ‘suitable measures’ to ensure the full implementation of that directive. Thus, the referring court concludes that national legislation allowing associations to bring legal proceedings in the interest of consumers may constitute such a ‘suitable measure’.  
36      That court notes, in this regard, that Article 80(2) of Regulation 2016/679, which repealed and replaced Directive 95/46, expressly authorises the bringing of legal proceedings by such an association, which would tend to confirm that the latter directive did not preclude such an action.  
37      Further, that court is uncertain whether the operator of a website, such as Fashion ID, that embeds on that website a social plugin allowing personal data to be collected can be considered to be a controller within the meaning of Article 2(d) of Directive 95/46 despite the latter having no control over the processing of the data transmitted to the provider of that plugin. In this context, the referring court refers to the case that gave rise to the judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
 (C-210/16, EU:C:2018:388), which dealt with a similar question.  
38      In the alternative, in the event that Fashion ID is not to be considered to be a controller, the referring court is uncertain whether that directive exhaustively regulates that notion, such that it precludes national legislation that establishes civil liability for a third party who infringes data protection rights. The referring court asserts that it would be possible to envisage Fashion ID being liable on this basis under national law as a ‘disrupter’ (‘  
Störer  
’).  
39      If Fashion ID had to be considered to be a controller or was at least liable as a ‘disrupter’ for any data protection infringements by Facebook Ireland, the referring court is uncertain whether the processing of the personal data at issue in the main proceedings is lawful and whether the duty to inform the data subject under Article 10 of Directive 95/46 rests with Fashion ID or with Facebook Ireland.  
40      Thus, first, with regard to the conditions for the lawfulness of the processing of data as provided for in Article 7(f) of Directive 95/46, the referring court expresses uncertainty as to whether, in a situation such as that at issue in the main proceedings, it is appropriate to take into account the legitimate interest of the operator of the website or that of the provider of the social plugin.  
41      Second, that court is unsure who is required to obtain the consent of and inform the data subjects whose personal data are processed in a situation such as that at issue in the main proceedings. The referring court takes the view that the matter of who is obliged to inform the persons concerned, as provided for in Article 10 of Directive 95/46, is particularly important given that any embedding of third-party content on a website gives rise, in principle, to the processing of personal data, the scope and purpose of which are, however, unknown to the person embedding that content, namely the operator of the website concerned. That operator could not, therefore, provide the information required, to the extent that it is required to, meaning that the imposition of an obligation on the operator to inform the data subjects would, in practice, amount to a prohibition on the embedding of third-party content.  
42      In those circumstances, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Do the rules in Articles 22, 23 and 24 of Directive [95/46] preclude national legislation which, in addition to the powers of intervention conferred on the data-protection authorities and the remedies available to the data subject, grants public-service associations the power to take action against the infringer in the event of an infringement in order to safeguard the interests of consumers?  
If Question 1 is answered in the negative:  
(2)      In a case such as the present one, in which someone has embedded a programming code in his website which causes the user’s browser to request content from a third party and, to this end, transmits personal data to the third party, is the person embedding the content the “controller” within the meaning of Article 2(d) of Directive [95/46] if that person is himself unable to influence this data-processing operation?  
(3)      If Question 2 is answered in the negative: Is Article 2(d) of Directive [95/46] to be interpreted as meaning that it definitively regulates liability and responsibility in such a way that it precludes civil claims against a third party who, although not a “controller”, nonetheless creates the cause for the processing operation, without influencing it?  
(4)      Whose “legitimate interests”, in a situation such as the present one, are the decisive ones in the balancing of interests to be undertaken pursuant to Article 7(f) of Directive [95/46]? Is it the interests in embedding third-party content or the interests of the third party?  
(5)      To whom must the consent to be declared under Articles 7(a) and 2(h) of Directive [95/46] be given in a situation such as that in the present case?  
(6)      Does the duty to inform under Article 10 of Directive [95/46] also apply in a situation such as that in the present case to the operator of the website who has embedded the content of a third party and thus creates the cause for the processing of personal data by the third party?’  
   
Consideration of the questions referred  
   
The first question  
43      By its first question the referring court asks, in essence, whether Articles 22 to 24 of Directive 95/46 must be interpreted as precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the laws protecting personal data.  
44      As a preliminary point, it should be noted that, under Article 22 of Directive 95/46, Member States are required to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.  
45      The third indent of Article 28(3) of Directive 95/46 states that a supervisory authority that is responsible under Article 28(1) of that directive for monitoring the application within the territory of a Member State of the provisions adopted by that Member State pursuant to that directive is endowed with, inter alia, the power to engage in legal proceedings where the national provisions adopted pursuant to that directive have been violated or to bring those violations to the attention of the judicial authorities.  
46      Article 28(4) of Directive 95/46 provides that a supervisory authority is to hear claims lodged by an association representing a data subject, within the meaning of Article 2(a) of that directive, concerning the protection of his rights and freedoms in regard to the processing of personal data.  
47      However, no provision of that directive obliges Member States to provide, or expressly empowers them to provide, in their national law that an association can represent a data subject in legal proceedings or commence legal proceedings on its own initiative against the person allegedly responsible for an infringement of the laws protecting personal data.  
48      Nevertheless, it does not follow from the above that Directive 95/46 precludes national legislation allowing consumer-protection associations to bring or defend legal proceedings against the person allegedly responsible for such an infringement.  
49      Under the third paragraph of Article 288 TFEU, the Member States are required, when transposing a directive, to ensure that it is fully effective, but they retain a broad discretion as to the choice of ways and means of ensuring that it is implemented. That freedom of choice does not affect the obligation imposed on all Member States to which the directive is addressed to adopt all the measures necessary to ensure that the directive concerned is fully effective in accordance with the objective which it seeks to attain (judgments of 6 October 2010,   
Base and Others  
, C-389/08, EU:C:2010:584, paragraphs 24 and 25, and of 22 February 2018,   
Porras Guisado  
, C-103/16, EU:C:2018:99, paragraph 57).  
50      In this regard, it must be noted that one of the underlying objectives of Directive 95/46 is to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data (see, to that effect, judgments of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 53, and of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraph 38). Recital 10 of Directive 95/46 adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection which they afford but must, on the contrary, seek to ensure a high level of protection in the European Union (judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 95, of 16 December 2008,   
Huber  
, C-524/06, EU:C:2008:724, paragraph 50, and of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 28).  
51      The fact that a Member State provides in its national legislation that it is possible for a consumer-protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data in no way undermines the objectives of that protection and, in fact, contributes to the realisation of those objectives.  
52      Nevertheless, Fashion ID and Facebook Ireland submit that, since Directive 95/46 fully harmonised national provisions on data protection, any legal proceedings not expressly provided for by that directive are precluded. They argue that Articles 22, 23 and 28 of Directive 95/46 provide for legal proceedings brought only by data subjects and data protection supervisory authorities.  
53      That argument, however, cannot be accepted.  
54      Directive 95/46 does indeed amount to a harmonisation of national legislation on the protection of personal data that is generally complete (see, to that effect, judgments of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 29, and of 7 November 2013,   
IPI  
, C-473/12, EU:C:2013:715, paragraph 31).  
55      The Court has thus held that Article 7 of that directive sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful and that Member States cannot add new principles relating to the lawfulness of the processing of personal data to that article or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article (judgments of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraphs 30 and 32, and of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 57).  
56      The Court has, however, also held that Directive 95/46 lays down rules that are relatively general since it has to be applied to a large number of very different situations. Those rules have a degree of flexibility and, in many instances, leave to the Member States the task of deciding the details or choosing between options, meaning that, in many respects, Member States have a margin of discretion in implementing that directive (see, to that effect, judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraphs 83, 84 and 97, and of 24 November 2011,   
Asociación Nacional de Establecimientos Financieros de Crédito  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 35).  
57      This is also the case for Articles 22 to 24 of Directive 95/46, which, as the Advocate General noted in point 42 of his Opinion, are worded in general terms and do not amount to an exhaustive harmonisation of the national provisions stipulating the judicial remedies that can be brought against a person allegedly responsible for an infringement of the laws protecting personal data (see, by analogy, judgment of 26 October 2017,   
I  
, C-195/16, EU:C:2017:815, paragraphs 57 and 58).  
58      In particular, although Article 22 of that directive requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the personal data processing in question, that directive does not, however, contain any provisions specifically governing the conditions under which that remedy may be exercised (see, to that effect, judgment of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraphs 54 and 55).  
59      In addition, Article 24 of Directive 95/46 provides that Member States are to adopt ‘suitable measures’ to ensure the full implementation of the provisions of that directive, without defining such measures. It seems that a provision making it possible for a consumer-protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data may constitute a suitable measure, within the meaning of that provision, that contributes, as observed in paragraph 51 above, to the realisation of the objectives of that directive, in accordance with the Court’s case-law (see, to that effect, judgment of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 97).  
60      Moreover, contrary to what is claimed by Fashion ID, the fact that a Member State can provide for such a possibility in its national legislation does not appear to be such as to undermine the independence with which the supervisory authorities must perform the functions entrusted to them under Article 28 of Directive 95/46, since that possibility affects neither those authorities’ freedom to take decisions nor their freedom to act.  
61      In addition, although it is true that Directive 95/46 does not appear among the measures listed in Annex I to Directive 2009/22, the fact nonetheless remains that, under Article 7 of the latter directive, that directive did not provide for an exhaustive harmonisation in that respect.  
62      Last, the fact that Regulation 2016/679, which repealed and replaced Directive 95/46 and has been applicable since 25 May 2018, expressly authorises, in Article 80(2) thereof, Member States to allow consumer-protection associations to bring or defend legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data does not mean that Member States could not grant them that right under Directive 95/46, but confirms, rather, that the interpretation of that directive in the present judgment reflects the will of the EU legislature.  
63      In the light of all the findings above, the answer to the first question is that Articles 22 to 24 of Directive 95/46 must be interpreted as not precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data.  
   
The second question  
64      By its second question, the referring court asks, in essence, whether the operator of a website, such as Fashion ID, that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46, despite that operator being unable to influence the processing of the data transmitted to that provider as a result.  
65      In this regard, it should be noted that, in accordance with the aim pursued by Directive 95/46, namely to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data, Article 2(d) of that directive defines the concept of ‘controller’ broadly as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (see, to that effect, judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraphs 26 and 27).  
66      As the Court has held previously, the objective of that provision is to ensure, through a broad definition of the concept of ‘controller’, effective and complete protection of data subjects (judgments of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 34, and of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 28).  
67      Furthermore, since, as Article 2(d) of Directive 95/46 expressly provides, the concept of ‘controller’ relates to the entity which ‘alone or jointly with others’ determines the purposes and means of the processing of personal data, that concept does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data-protection provisions (see, to that effect, judgments of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 29, and of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 65).  
68      The Court has also held that a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46 (judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 68).  
69      Furthermore, the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned (see, to that effect, judgments of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 38, and of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 69).  
70      That said, since the objective of Article 2(d) of Directive 95/46 is to ensure, through a broad definition of the concept of ‘controller’, the effective and comprehensive protection of the persons concerned, the existence of joint liability does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the particular case (see, to that effect, judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 66).  
71      In this regard, it should be pointed out, first, that Article 2(b) of Directive 95/46 defines ‘processing of personal data’ as ‘any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction’.  
72      It is apparent from that definition that the processing of personal data may consist in one or a number of operations, each of which relates to one of the different stages that the processing of personal data may involve.  
73      Second, it follows from the definition of the concept of ‘controller’ in Article 2(d) of Directive 95/46 that, as is noted in paragraph 65 above, where several operators determine jointly the purposes and means of the processing of personal data, they participate in that processing as controllers.  
74      Accordingly, as the Advocate General noted, in essence, in point 101 of his Opinion, it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means. By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means.  
75      In this case, subject to the investigations that it is for the referring court to carry out, it is apparent from the documents before the Court that, by embedding on its website the Facebook ‘Like’ button, Fashion ID appears to have made it possible for Facebook Ireland to obtain personal data of visitors to its website and that such a possibility is triggered as soon as the visitor consults that website, regardless of whether or not the visitor is a member of the social network Facebook, has clicked on the Facebook ‘Like’ button or is aware of such an operation.  
76      In view of that information, it should be pointed out that the operations involving the processing of personal data in respect of which Fashion ID is capable of determining, jointly with Facebook Ireland, the purposes and means are, for the purposes of the definition of the concept of ‘processing of personal data’ in Article 2(b) of Directive 95/46, the collection and disclosure by transmission of the personal data of visitors to its website. By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d).  
77      With regard to the means used for the purposes of the collection and disclosure by transmission of certain personal data of visitors to its website, it is apparent from paragraph 75 above that Fashion ID appears to have embedded on its website the Facebook ‘Like’ button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook.  
78      Moreover, by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin.  
79      In these circumstances, and subject to the investigations that it is for the referring court to carry out in this respect, it must be concluded that Facebook Ireland and Fashion ID determine jointly the means at the origin of the operations involving the collection and disclosure by transmission of the personal data of visitors to Fashion ID’s website.  
80      As to the purposes of those operations involving the processing of personal data, it appears that Fashion ID’s embedding of the Facebook ‘Like’ button on its website allows it to optimise the publicity of its goods by making them more visible on the social network Facebook when a visitor to its website clicks on that button. The reason why Fashion ID seems to have consented, at least implicitly, to the collection and disclosure by transmission of the personal data of visitors to its website by embedding such a plugin on that website is in order to benefit from the commercial advantage consisting in increased publicity for its goods; those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID.  
81      In such circumstances, it can be concluded, subject to the investigations that it is for the referring court to perform, that Fashion ID and Facebook Ireland determine jointly the purposes of the operations involving the collection and disclosure by transmission of the personal data at issue in the main proceedings.  
82      Further, as is apparent from the case-law referred to in paragraph 69 above, the fact that the operator of a website, such as Fashion ID, does not itself have access to the personal data collected and transmitted to the provider of the social plugin with which it determines jointly the means and purposes of the processing of personal data does not preclude it from being a controller within the meaning of Article 2(d) of Directive 95/46.  
83      Moreover, it must be emphasised that a website, such as that of Fashion ID, is visited both by those who are members of the social network Facebook, and who therefore have an account on that social network, and by those who do not have one. In that latter case, the responsibility of the operator of a website, such as Fashion ID, for the processing of the personal data of those persons appears to be even greater, as the mere consultation of such a website featuring the Facebook ‘Like’ button appears to trigger the processing of their personal data by Facebook Ireland (see, to that effect. judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 41).  
84      Accordingly, it seems that Fashion ID can be considered to be a controller within the meaning of Article 2(d) of Directive 95/46, jointly with Facebook Ireland, in respect of the operations involving the collection and disclosure by transmission of the personal data of visitors to its website.  
85      In the light of the findings above, the answer to the second question is that the operator of a website, such as Fashion ID, that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46. That liability is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue.  
   
The third question  
86      In view of the answer given to the second question, there is no need to answer the third question.  
   
The fourth question  
87      By its fourth question, the referring court asks, in essence, whether, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, it is appropriate, for the purposes of the application of Article 7(f) of Directive 95/46, to take into consideration a legitimate interest pursued by that operator or a legitimate interest pursued by that provider.  
88      As a preliminary point, it should be noted that, according to the Commission, this question is irrelevant for the resolution of the dispute in the main proceedings, since consent was not obtained from the data subjects as is required by Article 5(3) of Directive 2002/58.  
89      In that regard, it should be pointed out that Article 5(3) of Directive 2002/58 provides that Member States are to ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is allowed only on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46, inter alia, about the purposes of the processing.  
90      It is for the referring court to investigate whether, in a situation such as that at issue in the main proceedings, the provider of a social plugin, such as Facebook Ireland, gains access, as is maintained by the Commission, from the operator of the website to information stored in the terminal equipment, within the meaning of Article 5(3) of Directive 2002/58, of a visitor to that website.  
91      In such circumstances, and since the referring court seems to have concluded that, in the present case, the data transmitted to Facebook Ireland are personal data, within the meaning of Directive 95/46, which, moreover, are not necessarily limited to information stored in the terminal equipment, which it is for that court to confirm, the Commission’s views are insufficient to call into question the relevance of the fourth question referred for the resolution of the dispute in the main proceedings, which concerns the potentially lawful processing of the data at issue in the main proceedings, as was pointed out by the Advocate General in point 115 of his Opinion.  
92      Consequently, it is necessary to examine what legitimate interest must be taken into account for the purposes of the application of Article 7(f) of that directive to the processing of those data.  
93      In this regard, it should be noted at the outset that, according to the provisions of Chapter II of Directive 95/46, headed ‘General rules on the lawfulness of the processing of personal data’, subject to the derogations permitted under Article 13 of that directive, all processing of personal data must comply, inter alia, with one of the criteria for making data processing legitimate listed in Article 7 of that directive (see, to that effect, judgments of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 71, and of 1 October 2015,   
Bara and Others  
, C-201/14, EU:C:2015:638, paragraph 30).  
94      Under Article 7(f) of Directive 95/46, the interpretation of which is sought by the referring court, personal data may be processed if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1) of Directive 95/46.  
95      Article 7(f) of that directive thus lays down three cumulative conditions for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence (judgment of 4 May 2017,   
Rīgas satiksme  
, C-13/16, EU:C:2017:336, paragraph 28).  
96      Given that, in the light of the answer to the second question, it seems that, in a situation such as that at issue in the main proceedings, the operator of a website that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller responsible, jointly with that provider, for operations involving the processing of the personal data of visitors to its website in the form of collection and disclosure by transmission, it is necessary that each of those controllers should pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46, through those processing operations in order for those operations to be justified in respect of each of them.  
97      In the light of the findings above, the answer to the fourth question is that, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, it is necessary that that operator and that provider each pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46, through those processing operations in order for those operations to be justified in respect of each of them.  
   
The fifth and sixth questions  
98      By its fifth and sixth questions, which it is appropriate to examine together, the referring court wishes to know, in essence, first, whether Article 2(h) and Article 7(a) of Directive 95/46 must be interpreted as meaning that, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, the consent referred to in those provisions must be obtained by that operator or by that provider and, second, whether Article 10 of that directive must be interpreted as meaning that, in such a situation, the duty to inform provided for in that provision is incumbent on that operator.  
99      As is apparent from the answer to the second question, the operator of a website that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46, despite that liability being limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means.  
100    It thus appears that the duties that may be incumbent on that controller under Directive 95/46, such as the duty to obtain the consent of the data subject under Article 2(h) and Article 7(a) of that directive and the duty to inform under Article 10 thereof, must relate to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means.  
101    In the present case, while the operator of a website that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller, jointly with that provider, in respect of operations involving the collection and disclosure by transmission of the personal data of that visitor, its duty to obtain the consent from the data subject under Article 2(h) and Article 7(a) of Directive 95/46 and its duty to inform under Article 10 of that directive relate only to those operations. By contrast, those duties do not cover operations involving the processing of personal data at other stages occurring before or after those operations which involve, as the case may be, the processing of personal data at issue.  
102    With regard to the consent referred to in Article 2(h) and Article 7(a) of Directive 95/46, it appears that such consent must be given prior to the collection and disclosure by transmission of the data subject’s data. In such circumstances, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data. As the Advocate General noted in point 132 of his Opinion, it would not be in line with efficient and timely protection of the data subject’s rights if the consent were given only to the joint controller that is involved later, namely the provider of that plugin. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means.  
103    The same applies in regard to the duty to inform under Article 10 of Directive 95/46.  
104    In that regard, it follows from the wording of that provision that the controller or his representative must provide, as a minimum, the information referred to in that provision to the subject whose data are being collected. It thus appears that that information must be given by the controller immediately, that is to say, when the data are collected (see, to that effect, judgments of 7 May 2009,   
Rijkeboer  
, C-553/07, EU:C:2009:293, paragraph 68, and of 7 November 2013,   
IPI  
, C-473/12, EU:C:2013:715, paragraph 23).  
105    It follows that, in a situation such as that at issue in the main proceedings, the duty to inform under Article 10 of Directive 95/46 is incumbent also on the operator of the website, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means.  
106    In the light of the findings above, the answer to the fifth and sixth questions is that Article 2(h) and Article 7(a) of Directive 95/46 must be interpreted as meaning that, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, the consent referred to in those provisions must be obtained by that operator only with regard to the operation or set of operations involving the processing of personal data in respect of which that operator determines the purposes and means. In addition, Article 10 of that directive must be interpreted as meaning that, in such a situation, the duty to inform laid down in that provision is incumbent also on that operator, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means.  
   
Costs  
107    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
1.        
Articles 22 to 24 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as not precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data.  
2.        
The operator of a website, such as Fashion ID GmbH & Co. KG, that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46. That liability is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue.  
3.        
In a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, it is necessary that that operator and that provider each pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46, through those processing operations in order for those operations to be justified in respect of each of them.  
4.        
Article 2(h) and Article 7(a) of Directive 95/46 must be interpreted as meaning that, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, the consent referred to in those provisions must be obtained by that operator only with regard to the operation or set of operations involving the processing of personal data in respect of which that operator determines the purposes and means. In addition, Article 10 of that directive must be interpreted as meaning that, in such a situation, the duty to inform laid down in that provision is incumbent also on that operator, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means.

ID: 847fbb68-25c5-4b44-ae35-541d172c9267

of 7 Mar 2024, C-604/22 (  
IAB Europe  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Joint controllers   
   
JUDGMENT OF THE COURT (Fourth Chamber)  
7 March 2024 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Standard-setting sectoral organisation proposing to its members rules on the processing of users’ consent – Article 4(1) – Concept of ‘personal data’ – String of letters and characters capturing, in a structured and machine-readable manner, the preferences of an internet user relating to the consent of that user to the processing of his or her personal data – Article 4(7) – Concept of ‘controller’ – Article 26(1) – Concept of ‘joint controllers’ – Organisation which does not itself have access to the personal data processed by its members – Responsibility of the organisation extending to the subsequent processing of data carried out by third parties)  
In Case C-604/22,  
REQUEST for a preliminary ruling under Article 267 TFEU from the hof van beroep te Brussel (Court of Appeal, Brussels, Belgium), made by decision of 7 September 2022, received at the Court on 19 September 2022, in the proceedings  
IAB Europe  
v  
Gegevensbeschermingsautoriteit,  
interveners:  
Jef Ausloos,  
Pierre Dewitte,  
Johnny Ryan,  
Fundacja Panoptykon,  
Stichting Bits of Freedom,  
Ligue des Droits Humains VZW,  
THE COURT (Fourth Chamber),  
composed of C. Lycourgos, President of the Chamber, O. Spineanu-Matei, J.-C. Bonichot, S. Rodin and L.S. Rossi (Rapporteur), Judges,  
Advocate General: T. Ćapeta,  
Registrar: A. Lamote, Administrator,  
having regard to the written procedure and further to the hearing on 21 September 2023,  
after considering the observations submitted on behalf of:  
–        IAB Europe, by P. Craddock, avocat, and K. Van Quathem, advocaat,  
–        the Gegevensbeschermingsautoriteit, by E. Cloots, J. Roets and T. Roes, advocaten,  
–        Jef Ausloos, Pierre Dewitte, Johnny Ryan, Fundacja Panoptykon, Stichting Bits of Freedom and Ligue des Droits Humains VZW, by F. Debusseré and R. Roex, advocaten,  
–        the Austrian Government, by J. Schmoll and C. Gabauer, acting as Agents,  
–        the European Commission, by A. Bouchagiar and H. Kranenborg, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 4(1) and (7) and Article 24(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’), read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between IAB Europe and the Gegevensbeschermingsautoriteit (Data Protection Authority, Belgium; ‘the DPA’) concerning a decision of the Litigation Chamber of the DPA adopted against IAB Europe with regard to the alleged infringement of several provisions of the GDPR.  
   
Legal context  
   
European Union law  
3        Recitals 1, 10, 26 and 30 of the GDPR are worded as follows:  
‘(1)      The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the [Charter] and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.  
…  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
…  
(26)      The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.  
…  
(30)      Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.’  
4        Article 1 of the GDPR, entitled ‘Subject matter and objectives’, provides, in paragraph 2 thereof:  
‘This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.’  
5        Article 4 of that regulation provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;  
…  
(11)      “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;  
…’  
6        Article 6 of the GDPR, entitled ‘Lawfulness of processing’, is worded as follows:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.  
…’  
7        Article 24 of that regulation, entitled ‘Responsibility of the controller’, provides, in paragraph 1 thereof:  
‘Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.’  
8        Article 26 of that regulation, entitled ‘Joint controllers’, states, in paragraph 1 thereof:  
‘Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. …’  
9        Chapter VI of the GDPR, relating to ‘Independent supervisory authorities’, comprises Articles 51 to 59 of that regulation.  
10      Article 51 of that regulation, entitled ‘Supervisory authority’, provides, in paragraphs 1 and 2 thereof:  
‘1.      Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union …  
2.      Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the [European] Commission in accordance with Chapter VII.’  
11      According to Article 55(1) and (2) of the GDPR, entitled ‘Competence’:  
‘1.      Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.  
2.      Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.’  
12      Article 56 of that regulation, entitled ‘Competence of the lead supervisory authority’, states, in paragraph 1 thereof:  
‘Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.’  
13      Article 57 of the GDPR, entitled ‘Tasks’, provides, in paragraph 1 thereof:  
‘Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:  
(a)      monitor and enforce the application of this Regulation;  
…  
(g)      cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;  
…’  
14      Section 1, entitled ‘Cooperation’, of Chapter VII of the GDPR, entitled ‘Cooperation and consistency’, comprises Articles 60 to 62 of that regulation. Article 60, relating to ‘Cooperation between the lead supervisory authority and the other supervisory authorities concerned’, provides, in paragraph 1 thereof:  
‘The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.’  
15      Article 61 of the GDPR, entitled ‘Mutual assistance’, states, in paragraph 1 thereof:  
‘Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.’  
16      Article 62 of that regulation, entitled ‘Joint operations of supervisory authorities’, provides, in paragraphs 1 and 2 thereof:  
‘1.      The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.  
2.      Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. …’  
17      Section 2, entitled ‘Consistency’, of Chapter VII of the GDPR comprises Articles 63 to 67 of that regulation. Article 63, entitled ‘Consistency mechanism’, is worded as follows:  
‘In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.’  
   
Belgian law  
18      The wet tot oprichting van de Gegevensbeschermingsautoriteit (Law establishing the Data Protection Authority), of 3 December 2017 (  
Belgisch Staatsblad  
, 10 January 2018, p. 989; ‘the LDPA’), provides, in point 9° of Article 100(1) thereof:  
‘The Litigation Chamber shall have the power to:  
…  
9°      order that the processing be brought into conformity’.  
19      Article 101 of the LDPA provides:  
‘The Litigation Chamber may decide to impose an administrative fine on the parties against whom proceedings are brought in accordance with the general principles referred to in Article 83 of [the GDPR].’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
20      IAB Europe is a non-profit association established in Belgium which represents undertakings in the digital advertising and marketing sector at European level. The members of IAB Europe are undertakings in that sector, such as publishers, e-commerce and marketing undertakings and intermediaries, as well as national associations, including national IAB (Interactive Advertising Bureau) branches, which, in turn, have undertakings in that sector as members. The members of IAB Europe include, inter alia, undertakings which generate significant income through the sale of advertising space on websites or applications.  
21      IAB Europe has drawn up the Transparency & Consent Framework (‘the TCF’), which is a framework of rules consisting of guidelines, instructions, technical specifications, protocols and contractual obligations that enable both the provider of a website or application and data brokers or indeed advertising platforms to process lawfully the personal data of a user of a website or application.  
22      The TCF is aimed, inter alia, at promoting compliance with the GDPR when those operators use the OpenRTB protocol, one of the most widely used protocols for Real Time Bidding, which is an instant and automated online auction system of user profiles for the purpose of selling and purchasing advertising space on the internet (‘RTB’). In the light of certain practices implemented by members of IAB Europe in the context of that mass personal data exchange system relating to user profiles, the TCF was presented by IAB Europe as a solution capable of bringing that auction system into conformity with the GDPR.  
23      In particular, as is apparent from the file submitted to the Court, from a technical point of view, when a user consults a website or application containing advertising space, advertising technology companies – particularly data brokers and advertising platforms, which represent thousands of advertisers – can bid in real time, behind the scenes, to acquire that advertising space by means of an automated auction system using algorithms, in order to display in that space targeted advertisements specifically tailored to the profile of such a user.  
24      However, before displaying such targeted advertisements, the prior consent of that user must be obtained. Thus, when he or she consults a website or application for the first time, a Consent Management Platform (‘CMP’) appears in a pop-up window enabling that user, first, to give his or her consent to the provider of the website or application for the collection and processing of his or her personal data for pre-defined purposes, such as, inter alia, marketing or advertising, or with a view to sharing those data with certain providers, and, second, to object to various types of data processing or to the sharing of those data, based on legitimate interests claimed by providers, within the meaning of Article 6(1)(f) of the GDPR. Those personal data relate, inter alia, to the user’s location, age and search and recent purchase history.  
25      In that context, the TCF provides a framework for large-scale processing of personal data and facilitates the recording of users’ preferences by means of the CMP. Those preferences are subsequently encoded and stored in a string composed of a combination of letters and characters referred to by IAB Europe as the Transparency and Consent String (‘the TC String’), which is shared with personal data brokers and advertising platforms participating in the OpenRTB protocol, so that they know to what the user has consented or objected. The CMP also places a cookie (euconsent-v2) on the user’s device. When they are combined, the TC String and the euconsent-v2 cookie can be linked to that user’s IP address.  
26      The TCF thus plays a role in the operation of the OpenRTB protocol, since it makes it possible to transcribe the user’s preferences with a view to communicating them to potential sellers and achieving various processing objectives, including the offering of tailored advertising. The TCF aims, inter alia, to guarantee to personal data brokers and advertising platforms, by means of the TC String, compliance with the GDPR.  
27      Since 2019, the DPA has received a number of complaints against IAB Europe, originating both from Belgium and from third countries, concerning the compliance of the TCF with the GDPR. After having examined those complaints, the DPA, in its capacity as lead supervisory authority within the meaning of Article 56(1) of the GDPR, triggered the cooperation and consistency mechanism, in accordance with Articles 60 to 63 of that regulation, in order to reach a common decision approved jointly by all 21 national supervisory authorities involved in that mechanism. Thus, by its decision of 2 February 2022 (‘the decision of 2 February 2022’), the Litigation Chamber of the DPA held that IAB Europe was acting as personal data controller as regards the recording of the consent signal, objections and preferences of individual users by means of a TC String, which, according to the Litigation Chamber of the DPA, is associated with an identifiable user. In addition, in that decision, the Litigation Chamber of the DPA ordered IAB Europe, in accordance with point 9° of Article 100(1) of the LDPA, to bring into conformity with the provisions of the GDPR the processing of personal data carried out in the context of the TCF and imposed on it a number of corrective measures as well as an administrative fine.  
28      IAB Europe brought an action against that decision before the referring court, the hof van beroep te Brussel (Court of Appeal, Brussels, Belgium). IAB Europe requests that court to annul the decision of 2 February 2022. It challenges, inter alia, the fact that it was considered to have acted as controller. It also submits that, in so far as the decision finds that the TC String is personal data within the meaning of Article 4(1) of the GDPR, that decision is insufficiently qualified and reasoned and that, in any event, it is incorrect. In particular, IAB Europe argues that only the other participants in the TCF could combine the TC String with an IP address to convert it into an item of personal data, that the TC String is not specific to a user and that IAB Europe does not have the possibility to access the data processed in that context by its members.  
29      The DPA, supported in the national proceedings by Mr Jef Ausloos, Mr Pierre Dewitte, Mr Johnny Ryan, Fundacja Panoptykon, Stichting Bits of Freedom and Ligue des Droits Humains VZW, contends, inter alia, that TC Strings do constitute personal data, in so far as CMPs can link TC Strings to IP addresses, that, moreover, participants in the TCF can also identify users on the basis of other data, that IAB Europe has access to the information needed to do that, and that such identification of the user is precisely the purpose of the TC String, which is intended to facilitate the sale of targeted advertising. In addition, the DPA maintains, inter alia, that the fact that IAB Europe must be regarded as a controller within the meaning of the GDPR is apparent from its decisive role in the processing of TC Strings. The DPA adds that IAB Europe determines, respectively, the purposes and means of the processing, how TC Strings are generated, modified and read, how and where the necessary cookies are stored, who receives the personal data and on the basis of which criteria the storage periods for TC Strings may be established.  
30      The referring court has doubts as to whether a TC String, be it combined with an IP address or not, constitutes personal data and, if so, whether IAB Europe must be classified as a personal data controller in the context of the TCF, in particular with regard to the processing of the TC String. In that respect, the referring court states that, while it is true that the decision of 2 February 2022 reflects the common position adopted jointly by the various national supervisory authorities involved in the present case, the Court of Justice has not yet had the opportunity to rule on that new and far-reaching technology which the TC String represents.  
31      In those circumstances, the hof van beroep te Brussel (Court of Appeal, Brussels) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      (a)      Must Article 4(1) of [the GDPR], read in combination with Articles 7 and 8 of the [Charter], be interpreted as meaning that a character string that captures the preferences of an [internet] user in connection with the processing of his or her personal data in a structured and machine-readable manner constitutes personal data within the meaning of [that] provision in respect of [(i)] a sectoral organisation which makes available to its members a standard whereby it prescribes to them how that string should be generated, stored and/or distributed practically and technically, and [(ii)] the parties that have implemented that standard on their websites or in their apps and thus have access to that string?  
(b)      Does it make a difference in that regard if the implementation of the standard means that [that] string is available together with an IP address?  
(c)      Does the answer to questions 1(a) and 1(b) lead to a different conclusion if [that] standard-setting sectoral organisation does not itself have legal access to the personal data that are processed within [that] standard by its members?  
(2)      (a)      Must [Article] 4(7) and [Article] 24(1) of [the GDPR], read in combination with Articles 7 and 8 of the [Charter], be interpreted as meaning that a standard-setting sectoral organisation must be classified as a controller if it offers its members a standard for managing consent which contains, in addition to a binding technical framework, rules setting out in detail how those consent data – which constitute personal data – must be stored and disseminated?  
(b)      Does the answer to question 2(a) lead to a different conclusion if [that] sectoral organisation … does not itself have legal access to the personal data that are processed within [that] standard by its members?  
(c)      If the standard-setting sectoral organisation must be designated as a controller or a joint controller for the processing of [internet] users’ preferences, does that (joint) responsibility of the standard-setting sectoral organisation therefore automatically extend to the subsequent processing by third parties for which the [internet] users’ preferences were obtained, such as targeted online advertising by publishers and vendors?’  
   
The first question  
32      By its first question, the referring court asks, in essence, whether Article 4(1) of the GDPR must be interpreted as meaning that a string composed of a combination of letters and characters, such as the TC String, containing the preferences of a user of the internet or of an application relating to that user’s consent to the processing of personal data concerning him or her by website or application providers as well as by brokers of such data and by advertising platforms, constitutes personal data within the meaning of that provision, where a sectoral organisation has established the framework of rules under which that string must be generated, stored or disseminated and the members of such an organisation have implemented such rules and thus have access to that string. That court also wishes to ascertain whether, for the purpose of answering that question, it is important, in the first place, for that string to be associated with an identifier, such as, inter alia, the IP address of that user’s device, allowing the data subject to be identified, and, in the second place, for such a sectoral organisation to have the right to access directly the personal data which are processed by its members under the framework of rules that it has established.  
33      As a preliminary point, it should be recalled that, since the GDPR repealed and replaced Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) and the relevant provisions of that regulation have essentially the same scope as that of the relevant provisions of that directive, the Court’s case-law on that directive is also applicable, in principle, to that regulation (judgment of 17 June 2021,   
M.I.C.M.  
, C-597/19, EU:C:2021:492, paragraph 107).  
34      It should also be borne in mind that, according to settled case-law, the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 22 June 2023,   
Pankki S  
, C-579/21, EU:C:2023:501, paragraph 38 and the case-law cited).  
35      In that regard, it should be noted that Article 4(1) of the GDPR states that personal data is ‘any information relating to an identified or identifiable natural person’, and specifies that ‘an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.  
36      The use of the expression ‘any information’ in the definition of the concept of ‘personal data’ in that provision reflects the aim of the EU legislature to assign a wide scope to that concept, which potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it ‘relates to’ the data subject (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 23 and the case-law cited).  
37      In that regard, the Court has held that information relates to an identified or identifiable natural person where, by reason of its content, purpose or effect, it is linked to an identifiable person (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 24 and the case-law cited).  
38      As regards the ‘identifiable’ nature of a person, it is clear from the wording of Article 4(1) of the GDPR that an identifiable person is one who can be identified not only directly, but also indirectly.  
39      As the Court has already held, the use by the EU legislature of the word ‘indirectly’ suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified (see, by analogy, judgment of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 41). On the contrary, it follows from Article 4(5) of the GDPR, read in conjunction with recital 26 of that regulation, that personal data which could be attributed to a natural person by the use of additional information must be considered to be information on an identifiable natural person (judgment of 5 December 2023,   
Nacionalinis visuomenės sveikatos centras  
, C-683/21, EU:C:2023:949, paragraph 58).  
40      Furthermore, that recital 26 states that, in order to determine whether a person is ‘identifiable’, account should be taken of ‘all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly’. That wording suggests that, for information to be treated as ‘personal data’ within the meaning of Article 4(1) of that regulation, it is not required that all the information enabling the identification of the data subject must be in the hands of one person (see, by analogy, judgment of 19 October 2016,   
Breyer  
, C-582/14, EU:C:2016:779, paragraph 43).  
41      Therefore, the concept of ‘personal data’ covers not only data collected and stored by the controller, but also includes all information resulting from the processing of personal data relating to an identified or identifiable person (judgment of 22 June 2023,   
Pankki S  
, C-579/21, EU:C:2023:501, paragraph 45).  
42      In the present case, it should be noted that a string composed of a combination of letters and characters, such as the TC String, contains the preferences of a user of the internet or of an application relating to that user’s consent to the processing by third parties of personal data concerning him or her or relating to any objection by him or her to the processing of such data based on an alleged legitimate interest under Article 6(1)(f) of the GDPR.  
43      Even if a TC String did not itself contain factors allowing the data subject to be identified directly, it would still be the case, in the first place, that it contained the individual preferences of a specific user regarding his or her consent to the processing of personal data concerning him or her, that information ‘relating to [a] … natural person’ within the meaning of Article 4(1) of the GDPR.  
44      In the second place, it is also common ground that, where the information contained in a TC String is associated with an identifier, such as, inter alia, the IP address of the device of such a user, that information may make it possible to create a profile of that user and actually identify the person specifically concerned by such information.  
45      In so far as associating a string composed of a combination of letters and characters, such as the TC String, with additional data, inter alia with the IP address of a user’s device or with other identifiers, allows that user to be identified, it must be considered that the TC String contains information concerning an identifiable user and therefore constitutes personal data within the meaning of Article 4(1) of the GDPR, a conclusion which is supported by recital 30 of the GDPR, which expressly refers to such a case.  
46      That interpretation cannot be called into question by the mere fact that IAB Europe cannot itself combine the TC String with the IP address of a user’s device and does not have the possibility of directly accessing the data processed by its members in the context of the TCF.  
47      As is apparent from the case-law referred to in paragraph 40 above, such a fact does not preclude a TC String from being classified as ‘personal data’ within the meaning of Article 4(1) of the GDPR.  
48      Moreover, it is apparent from the documents before the Court, and in particular from the decision of 2 February 2022, that the members of IAB Europe are required to provide that organisation, at its request, with all the information allowing it to identify the users whose data are the subject of a TC String.  
49      It therefore appears, subject to the verifications which are for the referring court to carry out in that regard, that IAB Europe has, in accordance with what is stated in recital 26 of the GDPR, reasonable means allowing it to identify a particular natural person from a TC String, on the basis of the information which its members and other organisations participating in the TCF are required to provide to it.  
50      It follows from the foregoing that a TC String constitutes personal data within the meaning of Article 4(1) of the GDPR. It is irrelevant in that regard that, without an external contribution which it is entitled to require, such a sectoral organisation can neither access the data that are processed by its members under the rules which it has established nor combine the TC String with other identifiers, such as, inter alia, the IP address of a user’s device.  
51      In view of the foregoing, the answer to the first question is that Article 4(1) of the GDPR must be interpreted as meaning that a string composed of a combination of letters and characters, such as the TC String, containing the preferences of a user of the internet or of an application relating to that user’s consent to the processing of personal data concerning him or her by website or application providers as well as by brokers of such data and by advertising platforms constitutes personal data within the meaning of that provision in so far as, where those data may, by reasonable means, be associated with an identifier, such as, inter alia, the IP address of that user’s device, they allow the data subject to be identified. In such circumstances, the fact that, without an external contribution, a sectoral organisation holding that string can neither access the data that are processed by its members under the rules which that organisation has established nor combine that string with other factors does not preclude that string from constituting personal data within the meaning of that provision.  
   
The second question  
52      By its second question, the referring court asks, in essence, whether Article 4(7) of the GDPR must be interpreted as meaning that:  
–        first, a sectoral organisation, in so far as it proposes to its members a framework of rules that it has established relating to consent to the processing of personal data, which contains not only binding technical rules but also rules setting out in detail the arrangements for storing and disseminating personal data relating to such consent, must be classified as a ‘controller’ within the meaning of that provision, and whether, for the answer to that question, it is relevant that such a sectoral organisation itself have direct access to the personal data processed by its members under those rules;  
–        second, any joint controllership of that sectoral organisation extends automatically to the subsequent processing of personal data carried out by third parties, such as website or application providers, with regard to users’ preferences for the purposes of targeted online advertising.  
53      As a preliminary point, it should be borne in mind that the objective pursued by the GDPR, as is set out in Article 1 thereof and in recitals 1 and 10 thereof, consists, inter alia, in ensuring a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, as enshrined in Article 8(1) of the Charter and Article 16(1) TFEU (judgment of 4 May 2023,   
Bundesrepublik Deutschland (Court electronic mailbox)  
,  
 C-60/22, EU:C:2023:373, paragraph 64).  
54      In accordance with that objective, Article 4(7) of the GDPR defines broadly the concept of ‘controller’ as referring to the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.  
55      As the Court has previously held, the objective of that provision is to ensure, through that broad definition of the concept of ‘controller’, effective and complete protection of data subjects (see, by analogy, judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 28).  
56      Furthermore, since, as Article 4(7) of the GDPR expressly provides, the concept of ‘controller’ relates to the entity which ‘alone or jointly with others’ determines the purposes and means of the processing of personal data, that concept does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions (see, by analogy, judgments of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 29, and of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 65).  
57      The Court has also found that a natural or legal person who exerts influence over the processing of personal data, for his, her or its own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 4(7) of the GDPR (see, by analogy, judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 68). Thus, under Article 26(1) of the GDPR, ‘joint controllers’ exist where two or more controllers jointly determine the purposes and means of processing (judgment of 5 December 2023,   
Nacionalinis visuomenės sveikatos centras  
, C-683/21, EU:C:2023:949, paragraph 40).  
58      In that regard, although each joint controller must independently meet the definition of ‘controller’ which is set out in Article 4(7) of the GDPR, the existence of joint controllership does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed in the light of all the relevant circumstances of the particular case. In addition, the joint controllership of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned (see, by analogy, judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraphs 66 and 69 and the case-law cited).  
59      Participation in the determination of the purposes and means of processing can take different forms, since such participation can result from a common decision taken by two or more entities or from converging decisions of those entities. Where the latter is the case, those decisions must complement each other in such a manner that they each have a tangible impact on the determination of the purposes and means of the processing. By contrast, it cannot be required that there be a formal arrangement between those controllers as regards the purposes and means of processing (judgment of 5 December 2023,   
Nacionalinis visuomenės sveikatos centras  
, C-683/21, EU:C:2023:949, paragraphs 43 and 44).  
60      In the light of the foregoing, the first part of the second question referred must be regarded as seeking to ascertain whether a sectoral organisation, such as IAB Europe, may be regarded as a joint controller for the purposes of Article 4(7) and Article 26(1) of the GDPR.  
61      To that end, it is therefore necessary to assess whether, having regard to the particular circumstances of the case at issue, IAB Europe exerts influence over the processing of personal data, such as the TC String, for its own purposes, and determines, jointly with others, the purposes and means of such processing.  
62      As regards, in the first place, the purposes of such processing of personal data, subject to the verifications which are for the referring court to carry out, it is apparent from the documents before the Court that, as has been noted in paragraphs 21 and 22 above, the TCF established by IAB Europe constitutes a framework of rules intended to ensure that the processing of personal data of a user of a website or application carried out by certain operators which participate in the online auctioning of advertising space is in compliance with the GDPR.  
63      In those circumstances, the TCF aims, in essence, to promote and enable the sale and purchase of advertising space on the internet by such operators.  
64      Accordingly, the view may be taken, subject to the verifications which are for the referring court to carry out, that IAB Europe exerts influence over the personal data processing operations at issue in the main proceedings, for its own purposes, and determines, as a result, jointly with its members, the purposes of such operations.  
65      In the second place, as regards the means employed for the purposes of such processing of personal data, it is apparent from the documents before the Court, subject to the verifications which are for the referring court to carry out, that the TCF constitutes a framework of rules which the members of IAB Europe are supposed to accept in order to join that association. In particular, as was confirmed by IAB Europe at the hearing before the Court, if one of its members does not comply with the rules of the TCF, IAB Europe may adopt a non-compliance and suspension decision in respect of that member, which may result in the exclusion of that member from the TCF and, consequently, prevent it from relying on the guarantee of GDPR compliance that that system is supposed to provide with regard to the processing of personal data which that member carries out using TC Strings.  
66      Furthermore, and from a practical point of view, as has been stated in paragraph 21 above, the TCF established by IAB Europe contains technical specifications relating to the processing of the TC String. In particular, it appears that those specifications describe precisely how CMPs are required to collect users’ preferences relating to the processing of personal data concerning those users and how such preferences must be processed in order to generate a TC String. Moreover, precise rules are also laid down as regards the content of the TC String as well as the storage and sharing thereof.  
67      It is apparent in particular from the decision of 2 February 2022 that IAB Europe prescribes, as part of those rules, inter alia the standardised manner in which the various parties involved in the TCF may consult the preferences, objections and consents of users contained in the TC Strings.  
68      In those circumstances, and subject to the verifications which are for the referring court to carry out, a sectoral organisation such as IAB Europe must be regarded as exerting influence over the personal data processing operations at issue in the main proceedings, for its own purposes, and determines, as a result, jointly with its members, the means behind such operations. It follows that such an organisation must be regarded as a ‘joint controller’, for the purposes of Article 4(7) and Article 26(1) of the GDPR, in accordance with the case-law referred to in paragraph 57 above.  
69      The fact, mentioned by the referring court, that such a sectoral organisation does not itself have direct access to the TC Strings or, therefore, to the personal data processed under the abovementioned rules by its members, with which it jointly determines the purposes and means of the processing of those data, does not, in accordance with the case-law referred to in paragraph 58 above, preclude it from being classified as a ‘controller’ within the meaning of those provisions.  
70      Furthermore, in response to the doubts expressed by that court, it can be ruled out that any joint controllership of that sectoral organisation extends automatically to the subsequent processing of personal data carried out by third parties, such as website or application providers, with regard to users’ preferences for the purposes of targeted online advertising.  
71      In that regard, it should be noted, first, that Article 4(2) of the GDPR defines the ‘processing’ of personal data as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’.  
72      It is clear from that definition that the processing of personal data may consist of one or more operations, each relating to a different stage of that processing.  
73      Second, as the Court has already held, it follows from Article 4(7) and Article 26(1) of the GDPR that a natural or legal person may be regarded as a joint controller in respect of personal data processing operations only where that person jointly determines the purposes and means of such operations. Therefore, and without prejudice to any civil liability provided for in national law in that respect, such a natural or legal person cannot be regarded as a controller, within the meaning of those provisions, in respect of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means (see, by analogy, judgment of 29 July 2019,   
Fashion ID  
, C-40/17, EU:C:2019:629, paragraph 74).  
74      In the present case, a distinction must be drawn between the processing of personal data carried out by the members of IAB Europe, namely website or application providers and data brokers or advertising platforms, when the consent preferences of the users concerned are recorded in a TC String in accordance with the framework of rules established in the TCF, on the one hand, and the subsequent processing of personal data carried out by those operators and by third parties on the basis of those preferences, such as the transmission of those data to third parties or the offering of personalised advertising to those users, on the other.  
75      That subsequent processing, subject to the verifications which are for the referring court to carry out, does not appear to involve the participation of IAB Europe, with the result that automatic responsibility on the part of such an organisation, held jointly with the abovementioned operators and with third parties, must be precluded in respect of the processing of personal data carried out on the basis of data relating to the preferences of the users concerned contained in a TC String.  
76      Accordingly, a sectoral organisation, such as IAB Europe, may be regarded as a controller in respect of such subsequent processing only where it is established that that organisation has exerted an influence over the determination of the purposes and means of that processing, which it is for the referring court to ascertain in the light of all the relevant circumstances of the case in the main proceedings.  
77      In view of all the foregoing considerations, the answer to the second question is that Article 4(7) and Article 26(1) of the GDPR must be interpreted as meaning that:  
–        first, a sectoral organisation, in so far as it proposes to its members a framework of rules that it has established relating to consent to the processing of personal data, which contains not only binding technical rules but also rules setting out in detail the arrangements for storing and disseminating personal data relating to such consent, must be classified as a ‘joint controller’ for the purpose of those provisions where, in the light of the particular circumstances of the individual case, it exerts influence over the personal data processing at issue, for its own purposes, and determines, as a result, jointly with its members, the purposes and means of such processing. The fact that such a sectoral organisation does not itself have direct access to the personal data processed by its members under those rules does not preclude it from holding the status of joint controller for the purpose of those provisions;  
–        second, the joint controllership of that sectoral organisation does not extend automatically to the subsequent processing of personal data carried out by third parties, such as website or application providers, with regard to users’ preferences for the purposes of targeted online advertising.  
   
Costs  
78      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Fourth Chamber) hereby rules:  
1.        
Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
must be interpreted as meaning that a string composed of a combination of letters and characters, such as the TC String (Transparency and Consent String), containing the preferences of a user of the internet or of an application relating to that user’s consent to the processing of personal data concerning him or her by website or application providers as well as by brokers of such data and by advertising platforms constitutes personal data within the meaning of that provision in so far as, where those data may, by reasonable means, be associated with an identifier, such as, inter alia, the IP address of that user’s device, they allow the data subject to be identified. In such circumstances, the fact that, without an external contribution, a sectoral organisation holding that string can neither access the data that are processed by its members under the rules which that organisation has established nor combine that string with other factors does not preclude that string from constituting personal data within the meaning of that provision.  
2.        
Article 4(7) and Article 26(1) of Regulation 2016/679  
must be interpreted as meaning that:  
–          
first, a sectoral organisation, in so far as it proposes to its members a framework of rules that it has established relating to consent to the processing of personal data, which contains not only binding technical rules but also rules setting out in detail the arrangements for storing and disseminating personal data relating to such consent, must be classified as a ‘joint controller’ for the purpose of those provisions where, in the light of the particular circumstances of the individual case, it exerts influence over the personal data processing at issue, for its own purposes, and determines, as a result, jointly with its members, the purposes and means of such processing. The fact that such a sectoral organisation does not itself have direct access to the personal data processed by its members under those rules does not preclude it from holding the status of joint controller for the purpose of those provisions;  
–          
second, the joint controllership of that sectoral organisation does not extend automatically to the subsequent processing of personal data carried out by third parties, such as website or application providers, with regard to users’ preferences for the purposes of targeted online advertising.

ID: 84a7c4f0-6035-44f6-9e77-0e3d953f7cd0

of 1 Jan 1970, C-350/21 (  
Spetsializirana prokuratura  
)  
  
  
  
  
Disclaimer

ID: 888c0a48-7424-4f16-a6f0-3aca84eb2c2c

of 27 Sep 2017, C-73/16 (  
Puškár  
)  
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness, fairness and transparency   
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accuracy   
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Integrity and confidentiality   
   
JUDGMENT OF THE COURT (Second Chamber)  
27 September 2017 (\*)  
(Reference for a preliminary ruling — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 1, 7 and 13 — Processing of personal data — Article 4(3) TEU — Drawing up of a list of personal data — Subject matter — Tax collection — Fight against tax fraud — Judicial review — Protection of fundamental rights and freedoms — Legal action dependent on a requirement of a prior administrative complaint — Whether that list is permissible as evidence — Rules on the lawfulness of the processing of personal data — Performance of a task carried out in the public interest by the controller)  
In Case C-73/16,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic), made by decision of 3 February 2016, received at the Court on 10 February 2016, in the proceedings  
Peter Puškár  
v  
Finančné riaditeľstvo Slovenskej republiky,  
Kriminálny úrad finančnej správy,  
THE COURT (Second Chamber),  
composed of M. Ilešič, President of the Chamber, A. Prechal, A. Rosas (Rapporteur), C. Toader and E. Jarašiūnas, Judges,  
Advocate General: J. Kokott,  
Registrar: M. Aleksejev, Administrator,  
having regard to the written procedure and further to the hearing on 16 February 2017,  
after considering the observations submitted on behalf of:  
–        Mr Puškár, by M. Mandzák, advokát,  
–        the Slovak Government, by B. Ricziová, acting as Agent,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the Spanish Government, by M.J. García-Valdecasas Dorrego, acting as Agent,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by P. Gentili, avvocato dello Stato,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the European Commission, by H. Krämer, A. Tokár and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 30 March 2017,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’), of Article 1(1), of Article 7(e) and of Article 13(1)(e) and (f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), and of Article 4(3) TEU and of Article 267 TFEU.  
2        The request has been made in proceedings between, on the one hand, Mr Peter Puškár and the Finančné riaditel’stvo Slovenskej republiky (Finance Directorate of the Slovak Republic, ‘the Finance Directorate’) and, on the other, the Kriminálny úrad finančnej správy (Financial Administration Criminal Office, Slovakia) concerning an action seeking to order the latter to remove Mr Puškár’s name from a list of persons considered by the Finance Directorate to be ‘front-men’, drawn up by the latter in the context of tax collection and the updating of which is carried out by the Finance Directorate, the tax offices subordinate to it and the Financial Administration Criminal Office (‘the contested list’).  
   
Legal context  
   
EU law  
3        Article 1 of Directive 95/46 provides:  
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
4        Article 2 of that directive provides:  
‘For the purposes of this Directive:  
(a)      “Personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;  
…’  
5        Article 3 of Directive 95/46, entitled ‘Scope’, provides:  
‘1.      This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
…’  
6        Article 6 of that directive provides:  
‘1.      Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purpose for which they were collected or for which they are further processed, are erased or rectified;  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States must lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
7        Article 7 of that directive is worded as follows:  
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent; or  
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject; or  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
8        Article 10 of Directive 95/46 provides:  
‘Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:  
(a)      the identity of the controller and of his representative, if any;  
(b)      the purposes of the processing operation for which the data are intended;  
(c)      any further information such as:  
–        the recipients or categories of recipients,  
–        whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,  
–        the existence of the right of access to and the right to rectify the data concerning him or her,  
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.’  
9        Article 11 of that directive states:  
‘1.      Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:  
(a)      the identity of the controller and of his representative, if any;  
(b)      the purposes of the processing;  
(c)      any further information such as:  
–        the categories of data concerned,  
–        the recipients or categories of recipients,  
–        the existence of the right of access to and the right to rectify the data concerning him or her,  
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.  
…’  
10      Article 12 of that directive provides:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
(a)      without constraint, at reasonable intervals and without excessive delay or expense:  
–        confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,  
–        communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,  
–        knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
(c)      notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.’  
11      Article 13(1) of Directive 95/46 provides:  
‘Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:  
…  
(c)      public security;  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
(e)      an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;  
(f)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);  
…’  
12      Article 14 of Directive 95/46 provides:  
‘Member States shall grant the data subject the right:  
(a)      at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;  
…’  
13      Article 17(1) of that directive provides as follows:  
‘1.      Member States shall provide that the controller must implement appropriate technical and organi[s]ational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.  
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.’  
14      Article 22 of the directive is worded as follows:  
‘Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.’  
15      Article 94 of the Rules of Procedure of the Court of Justice states:  
‘In addition to the text of the questions referred to the Court for a preliminary ruling, the request for a preliminary ruling shall contain:  
(a)      a summary of the subject-matter of the dispute and the relevant findings of fact as determined by the referring court or tribunal, or, at least, an account of the facts on which the questions are based;  
(b)      the tenor of any national provisions applicable in the case and, where appropriate, the relevant national case-law;  
(c)      a statement of the reasons which prompted the referring court or tribunal to inquire about the interpretation or validity of certain provisions of European Union law, and the relationship between those provisions and the national legislation applicable to the main proceedings.’  
   
Slovak law  
16      Article 19(3) of the Constitution of the Slovak Republic (‘the Constitution’), which forms part of the section entitled ‘Fundamental Principles’, provides:  
‘Everyone shall have the right to be protected against unjustified collection, disclosure and other misuse of his or her personal data.’  
17      Article 46(2) and (4) of the Constitution states:  
‘2. Any person who considers that the decision of a body of a public authority has adversely affected his rights may take legal action before the court or tribunal with jurisdiction so that it may review the legality of the decision unless otherwise provided for by law. However, review of decisions affecting fundamental rights and freedoms cannot be excluded from the jurisdiction of the court or tribunal.  
…  
4.      The conditions and procedures for judicial protection and all other forms of legal protection shall be established by law.’  
18      Paragraph 3(1) of Law No 9/2010 on Administrative Complaints reads as follows:  
‘An administrative complaint is an act by means of which an individual or a legal person …:  
(a)      asserts the protection of his rights or legally protected interests, which he considers to have been infringed by the activity or failure to act … of a body of public administration,  
(b)      alleges specific faults, in particular the infringement of legislation, which the body of public administration has the power to remedy.’  
19      The second sentence of Paragraph 135(1) of the Code of Civil Procedure, in the version applicable to the dispute in the main proceedings, provides:  
‘The court shall also be bound by any decision of the Ústavný súd [Slovenskej republiky] (Constitutional Court of the Slovak Republic) and of the European Court of Human Rights concerning fundamental human rights and freedoms.’  
20      Under Paragraph 250v(1) and (3) of the Code of Civil Procedure:  
‘1.      Individuals or legal persons who claim that their rights or legally protected interests have been harmed by the unlawful action of a public authority, which does not constitute a decision, and that they were the direct addressee of that action or that its effects directly prejudiced them, may apply for protection against the action before a court, provided such action or its effects persist or may recur.  
…  
3.      Legal proceedings shall be inadmissible unless the claimant has exhausted the remedies available to him under specific legislation …’  
21      Paragraph 164 of Law No 563/2009 on tax administration (‘the Tax Code’), in the version applicable to the case in the main proceedings, provides:  
‘For the purposes of tax administration, the tax authorities, Financial Directorate and Ministry of Finance shall be authorised to process the personal data of taxpayers, the representatives of taxpayers and other persons in accordance with specific legislation …; personal data may be made accessible only to the municipality in its capacity as the tax authorities, the Financial Administration and the Ministry of Finance and, in connection with tax administration and the performance of their tasks under specific legislation …, to any other person, court or prosecution authority. In the information systems … it is permissible to process the name and surname of an individual, his or her permanent address and, if he or she was not allocated a tax identification number on registration, his or her national identity number.’  
22      Paragraph 8 of Law No 479/2009 on State Administrative Bodies in the field of Taxes and Fees reads as follows:  
‘The Financial Directorate and Financial Administration shall be authorised to process personal data, in accordance with specific legislation … concerning individuals affected by acts adopted by the Financial Administration in connection with performance of its tasks under the present law or specific legislation; (1) the register of personal data is set out in the annex.’  
23      Paragraph 4(3)(d), (e) and (o) of Law No 333/2011 on State Administrative Bodies in the field of Taxes, Fees and Customs provides:  
‘3.      The Finance Directorate shall perform the following tasks:  
…  
(d)      it shall create, develop and operate the Financial Administration information systems … it shall notify to the Ministry of Finance its intention to carry out activities in relation to the creation and development of the Financial Administration information systems,  
(e)      it shall create and keep a central list of economic operators and other persons engaged in activities governed by the customs legislation and ensure that it is aligned with the relevant lists of the European Commission; it shall create and keep a central list of taxpayers and maintain and update the database; it shall create and keep that list through the Financial Administration information system,  
…  
(o)      it shall inform persons about their rights and obligations in matters concerning taxes and fees and their rights and obligations under specific legislation.’  
24      Pursuant to Paragraph 5(3) of Law 333/2011:  
‘The Financial Administration Criminal Office shall use the Financial Administration information systems, in which it shall collect, process, maintain, transfer, use, protect and delete information and personal data … about persons who have infringed the tax or customs legislation or who are suspected, on reasonable grounds, of infringing the tax or customs legislation, or persons who, within the Financial Administration’s field of jurisdiction, have undermined public order or who are suspected, on reasonable grounds, of undermining public order, and any other information on such infringements of the tax or customs legislation or undermining of public order; it shall provide or disclose that information and personal data to the Financial Directorate, the tax office or the customs office to the extent required for those bodies to carry out their tasks.’  
 The dispute in the main proceedings and the questions referred for a preliminary ruling  
25      Believing himself to be a victim of an infringement of his rights relating to personality by the inclusion of his name on the contested list, Mr Puškár applied to the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic), by an action of 9 January 2014, followed by an appeal of 19 November 2014, to order the Finance Directorate, all tax offices under its control and the Financial Administration Criminal Office not to include his name on the contested list or any other similar list and to delete any reference to him from those lists and from the finance authority’s IT system.  
26      According to Mr Puškár, the Finance Directorate and the Financial Administration Criminal Office have drawn up and are using the contested list, a list of natural persons, numbering 1 227 according to Mr Puškár, which the public authorities refer to by the expression ‘biele kone’ (‘white horses’). That expression is used for persons acting as ‘fronts’ in company director roles. Each natural person is, in principle, together with his national identity number and a tax identification number, associated with a legal person or legal persons — of which there are 3 369, according to Mr Puškár’s indications — within which he is deemed to be performing duties during a determined period.  
27      The referring court states that the existence of the contested list has been confirmed by the Financial Administration Criminal Office, which submits, however, that this list was drawn up by the Finance Directorate.  
28      According to the referring court, the contested list is protected against ‘unauthorised disclosure or access’ within the meaning of Article 17(1) of Directive 95/46, by appropriate technical and organisational measures. Nevertheless, neither in his pleadings nor at the hearing, did Mr Puškár claim that he had obtained the contested list with the consent legally required by the Finance Directorate or, where appropriate, the Financial Administration Criminal Office.  
29      It is apparent from the order for reference that the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) has dismissed as unfounded the actions brought by Mr Puškár and two other persons included on the contested list on procedural grounds, namely the fact that those applicants had not exhausted the remedies before the national administrative authorities, or on substantive grounds.  
30      Following the subsequent constitutional appeals lodged by Mr Puškár and those two other persons, the Ústavný súd Slovenskej republiky (Constitutional Court of the Slovak Republic), relying in particular on the case-law of the European Court of Human Rights, held that, in so doing, the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) had infringed several of those applicants’ fundamental rights, namely, inter alia, the right to a fair trial, the right to privacy as well as the right to the protection of personal data. Consequently, the Ústavný súd Slovenskej republiky (Constitutional Court of the Slovak Republic) set aside all of the judgments at issue of the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) and referred the cases back to that court so that it would rule again, reminding it that it was bound by the case-law of the European Court of Human Rights on the protection of personal data.  
31      According to the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic), the Ústavný súd Slovenskej republiky (Constitutional Court of the Slovak Republic) did not take into account the relevant case-law of the Court of Justice on the application of EU law on the protection of personal data.  
32      In those circumstances, the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Does Article 47(1) of the Charter, under which every person whose rights — including the right to privacy with respect to the processing of personal data in Article 1(1) et seq. of Directive 95/46 — are violated has the right to an effective remedy before a court in compliance with the conditions in Article 47 of the Charter, against a provision of national law which makes the exercise of an effective remedy before a court, meaning an administrative court, conditional on the fact that the claimant, to protect his rights and freedoms, must have previously exhausted the procedures available under   
lex specialis  
 — law on a specific subject — such as the Slovak Law on administrative complaints?  
(2)      Can the right to respect for private and family life, home and communications, in Article 7 of the Charter, and the right to the protection of personal data in Article 8 be interpreted to the effect that where there is an alleged violation of the right to the protection of personal data, which, with respect to the European Union, is implemented primarily through Directive 95/46, and under which, in particular  
–        the Member States must protect the right to privacy with respect to the processing of personal data (Article [1](1)), and  
–        the Member States are authorised to process personal data where this is necessary for the implementation of a task performed in the public interest (Article 7(e)) or is necessary for the purpose of a legitimate interests that is performed by the responsible authority or by the third party or parties to whom the data are disclosed, and  
–        a Member State is exceptionally authorised to limit obligations and rights (Article 13(1)(e) and (f)), where such a restriction is necessary to safeguard an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters,  
are interpreted in such a way as not to allow a Member State to create, without the consent of the person concerned, a list of personal data for the purposes of tax administration, so that the fact that personal data is made available to a public authority for the purpose of combating tax fraud in itself constitutes a risk?  
(3)      Can a list held by a financial authority of a Member State, which contains the claimant’s personal data and the inaccessibility of which has been secured by appropriate technical and organisational measures for the protection of personal data against unauthorised disclosure or access within the meaning of Article 17(1) of Directive 95/46, be regarded as unlawful evidence by virtue of the fact that it was obtained by the claimant without the lawful agreement of the relevant financial authority, which the referring court must refuse to admit in accordance with the requirements of EU law on a fair hearing in the second paragraph of Article 47(2) of the Charter?  
(4)      Is the abovementioned right to an effective legal remedy and to a fair hearing (in particular under Article 47 of the Charter) consistent with an approach taken by the referring court whereby, when, in this case, there is case-law from the European Court of Human Rights which differs from the answer obtained from the Court of Justice of the European Union, the referring court, in accordance with the principle of sincere cooperation in Article 4(3) TEU and Article 267 TFEU, gives precedence to the Court of Justice’s legal approach?’  
   
Consideration of the questions referred  
   
Preliminary observations  
33      It must be held at the outset, on the basis of the information provided by the referring court, that the data included on the contested list, namely, inter alia, the names of some natural persons, including Mr Puškár, are ‘personal data’ within the meaning of Article 2(a) of the Directive 95/46, since they are ‘information relating to an identified or identifiable natural person’ (see, to that effect, judgments of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 35, and of 1 October 2015,   
Bara and Others  
, C-201/14, EU:C:2015:638, paragraph 29).  
34      Both their collection and their use by the various tax authorities at issue in the case in the main proceedings therefore constitute ‘processing of personal data’ within the meaning of Article 2(b) of that directive (see, to that effect, judgments of 20 May 2003,   
Österreichischer Rundfunk and Others  
, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 64; of 16 December 2008,   
Huber  
, C-524/06, EU:C:2008:724, paragraph 43; and of 1 October 2015,   
Bara and Others  
, C-201/14, EU:C:2015:638, paragraph 29).  
35      The Spanish Government claims, however, that that processing of personal data is excluded from the scope of Directive 95/46 pursuant to the first indent of Article 3(2) thereof, under which that directive does not apply, in any case, to processing operations of personal data concerning public security, defence, State security, including the economic well-being of the State when the processing operation relates to State security matters, and the activities of the State in areas of criminal law.  
36      In that regard, it should be borne in mind that the activities which are mentioned by way of example in that article are, in any event, activities of the State or of State authorities unrelated to the fields of activity of individuals (see judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 43, and of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 41).  
37      The Court has also considered that the activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 are intended to define the scope of the exception which is provided for there, with the result that that exception applies only to the activities which are expressly listed there or which can be classified in the same category (see judgment of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 44).  
38      In so far as it renders inapplicable the system of protection of personal data provided for in Directive 95/46 and thus deviates from the objective underlying it, namely to ensure the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data, the exception provided for in the first indent of Article 3(2) of that directive must be interpreted strictly.  
39      In the case in the main proceedings it is apparent from the order for reference that the data at issue are collected and used for the purpose of collecting tax and combating tax fraud. Subject to the determinations to be carried out in that regard by the referring court, however, it does not appear that the processing of that data has as its object public security, defence or State security.  
40      Besides, even if it does not appear to be excluded that that data may be used in criminal proceedings which may be brought, in the event of an infringement in the field of taxation, against certain persons whose names are included in the contested list, the data at issue in the case in the main proceedings do not appear to have been collected for the specific purpose of the pursuit of such criminal proceedings or in the context of State activities relating to areas of criminal law.  
41      Moreover, it is clear from the case-law of the Court that tax data constitute ‘personal data’ within the meaning of Article 2(a) of Directive 95/46 (see, to that effect, judgment of 1 October 2015,   
Bara and Others  
, C-201/14, EU:C:2015:638, paragraph 29).  
42      In that context, it should be noted that Article 13(1)(e) of Directive 95/46 authorises the Member States to take legislative measures to limit the scope of the obligations and rights provided for in Article 6(1), Article 10, Article 11(1) and Articles 12 and 21 of that directive where such a restriction constitutes a measure necessary to safeguard an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters. A limitation of the data protection provided by Directive 95/46 for tax purposes is accordingly expressly provided for in that directive.  
43      Article 13(1) of Directive 95/46 necessarily presupposes that the national measures referred to therein, such as those necessary to safeguard an important economic or financial interest of a Member State in the field of taxation, fall within the scope of that directive (see, by analogy, judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 73).  
44      It follows from the foregoing that, subject to the determinations to be carried out by the referring court, processing of personal data, such as that at issue in the case in the main proceedings, falls within the scope of Directive 95/46.  
   
The first question  
45      By its first question, the referring court asks, in essence, whether Article 47 of the Charter must be interpreted as precluding national legislation, which makes the exercise of a judicial remedy by a person stating that his right to protection of personal data guaranteed by Directive 95/46 has been infringed, subject to the prior exhaustion of the remedies available to him before the national administrative authorities (‘the available administrative remedies’).  
   
Admissibility  
46      Mr Puškár and the Slovak Government dispute the admissibility of the first question referred.  
47      Mr Puškár claims, in particular, that that question is hypothetical in so far as, following the dismissal by the referring court of his first action on the ground that he had not lodged an administrative complaint, he had exhausted, prior to his second appeal before that court, all possible prior remedies.  
48      Similarly, the Slovak Government points out that the order for reference mentions at least two proceedings initiated by Mr Puškár, without specifying which of them is the subject of the present reference for a preliminary ruling. It claims that the information contained in the order for reference does not make it possible to determine whether a complaint had been lodged under Law No 9/2010, in which case the first question referred for a preliminary ruling would be inadmissible because of its hypothetical nature.  
49      In that regard, it must be borne in mind that, according to the Court’s settled case-law, in the context of the cooperation between the Court and the national courts provided for in Article 267 TFEU, it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions submitted concern the interpretation of EU law, the Court is, in principle, bound to give a ruling (see, in particular, judgment of 26 April 2017,   
Stichting Brein  
, C-527/15, EU:C:2017:300, paragraph 55 and the case-law cited).  
50      Questions on the interpretation of EU law referred by a national court in the factual and legislative context which that court is responsible for defining, and the accuracy of which is not a matter for the Court to determine, enjoy a presumption of relevance (see judgment of 17 July 2014,   
YS and Others  
, C-141/12 and C-372/12, EU:C:2014:2081, paragraph 63). The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought is unrelated to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see, in particular, judgment of 26 April 2017,   
Stichting Brein  
, C-527/15, EU:C:2017:300, paragraph 56 and the case-law cited).  
51      However, that is not the case here. As was pointed out in paragraphs 29 and 30 of the present judgment, it is clear from the order for reference that the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) had initially rejected the actions brought by Mr Puškár and two other persons on the ground, inter alia, that they had not exhausted the available administrative remedies, and that those decisions were annulled by the Ústavný súd Slovenskej republiky (Constitutional Court of the Slovak Republic).  
52      In those circumstances, it is not obvious that the interpretation of EU law sought by the referring court bears no relation to the actual facts of the main action or its purpose.  
53      It follows that the first question is admissible.  
   
Substance  
54      Article 22 of Directive 95/46 requires specifically that Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing of personal data in question.  
55      That directive, which does not contain any provisions governing specifically the conditions under which that remedy may be exercised, does not however exclude the possibility that national law may also establish remedies before the administrative authorities. On the contrary, it should be pointed out that Article 22 expressly states that it is ‘without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28 [of Directive 95/46], prior to referral to the judicial authority’, that Member States are to provide for the right of every person to that judicial remedy.  
56      However, it is necessary to determine whether Article 47 of the Charter precludes a Member State from providing that the exhaustion of available administrative remedies is a prerequisite for bringing such a judicial remedy.  
57      It should be recalled that, according to settled case-law of the Court, under the principle of sincere cooperation laid down in Article 4(3) TEU it is for the courts of the Member States to ensure judicial protection of a person’s rights under EU law, in addition, Article 19(1) TEU requiring Member States to provide remedies sufficient to ensure effective judicial protection in the fields covered by EU law (see, inter alia, judgments of 8 November 2016,   
Lesoochranárske zoskupenie VLK  
, C-243/15, EU:C:2016:838, paragraph 50, and of 26 July 2017,   
Sacko  
, C-348/16, EU:C:2017:591, paragraph 29).  
58      That requirement on the part of the Member States corresponds to the right enshrined in Article 47 of the Charter, entitled ‘Right to an effective remedy and to a fair trial’, which provides that everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal (see, to that effect, judgment of 16 May 2017,   
Berlioz Investment Fund  
, C-682/15, EU:C:2017:373, paragraph 44, and of 26 July 2017,   
Sacko  
, C-348/16, EU:C:2017:591, paragraph 30).  
59      It follows that, when they set out detailed procedural rules for legal actions intended to ensure the protection of rights conferred by Directive 95/46, the Member States must ensure compliance with the right to an effective remedy and to a fair hearing, enshrined in Article 47 of the Charter, which constitutes a reaffirmation of the principle of effective judicial protection (see, to that effect, judgments of 15 September 2016,   
Star Storage and Others  
, C-439/14 and C-488/14, EU:C:2016:688, paragraph 46, and of 26 July 2017,   
Sacko  
, C-348/16, EU:C:2017:591, paragraph 31).  
60      It follows that the characteristics of the remedy provided for in Article 22 of Directive 95/46 must be determined in a manner that is consistent with Article 47 of the Charter (see, by analogy, judgments of 17 December 2015,   
Tall  
, C-239/14, EU:C:2015:824, paragraph 51, and of 26 July 2017,   
Sacko  
, C-348/16, EU:C:2017:591, paragraph 31).  
61      In the present case, it is common ground in the case in the main proceedings that, by making the admissibility of a legal action brought by a person alleging infringement of his right to protection of personal data guaranteed by Directive 95/46 subject to the prior exhaustion of the administrative remedies available, the national legislation at issue introduces an additional step for access to the courts. As the Advocate General also stated in point 53 of her Opinion, such a procedural rule would delay access to a judicial remedy and could also cause additional costs to be incurred.  
62      The obligation to exhaust additional administrative remedies thereby constitutes, as a precondition for bringing a legal action, a limitation on the right to an effective remedy before a court within the meaning of Article 47 of the Charter which, in accordance with Article 52(1) of the Charter can therefore be justified only if it is provided for by law, if it respects the essence of that right and, subject to the principle of proportionality, if it is necessary and genuinely meets objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others (see, to that effect, judgment of 15 September 2016,   
Star Storage and Others  
, C-439/14 and C-488/14, paragraph 49).  
63      It must be held that, in the case in the main proceedings, it is clear from the order for reference that the legal basis for the obligation to exhaust available administrative remedies is set out in Paragraph 250v(3) of the Code of Civil Procedure, in such a way that it must be regarded as being provided for by national law (see, to that effect, judgment of 15 September 2016,   
Star Storage and Others  
, Case C-439/14 and C-488/14, paragraph 50 and the case-law cited).  
64      Moreover, that obligation respects the essential content of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. That obligation does not call into question that right as such. An additional procedural step is merely imposed in order to exercise it.  
65      Nonetheless, it must still be determined whether the obligation to exhaust available administrative remedies corresponds to an objective in the general interest and whether, in the affirmative, it complies with the principle of proportionality within the meaning of Article 52(1) of the Charter.  
66      It is clear from the order for reference and from the observations of the Slovak Government that the reasons for the mandatory introduction of an administrative complaint before bringing a legal action are linked, first, to the administrative authority, if it accepts the applicant’s arguments, to remedy more quickly an unlawful situation when it finds that the complaint is well founded, and to avoid seeing unexpected actions brought against that authority in court. Second, those reasons relate to the fact that such an obligation contributes to the efficiency of the judicial procedure where that authority does not share the applicant’s opinion and where the latter then lodges a legal action, because the judge can then rely on the existing administrative record.  
67      Thus it appears that the obligation to exhaust available administrative remedies is intended to relieve the courts of disputes which can be decided directly before the administrative authority concerned and to increase the efficiency of judicial proceedings as regards disputes in which a legal action is brought despite the fact that a complaint has already been lodged. The obligation therefore pursues legitimate general interest objectives.  
68      As is clear from point 62 of the Advocate General’s Opinion, the obligation to exhaust the available administrative remedies appears appropriate for achieving those objectives, no less onerous method than that obligation suggesting itself as capable of realising those objectives as efficiently.  
69      Moreover, it is not evident that any disadvantages caused by the obligation to exhaust available administrative remedies are clearly disproportionate to those objectives (see, by analogy, judgment of 18 March 2010,   
Alassini and Others  
, C-317/08 to C-320/08, EU:C:2010:146, paragraph 65).  
70      In that regard, it should be recalled that the Court held that the principle of effective judicial protection, reaffirmed in Article 47 of the Charter, did not preclude national legislation making the application of legal action in the field of electronic communications and consumer services subject to the prior implementation of out-of-court conciliation and mediation procedures provided that those procedures do not result in a decision which is binding on the parties, that they do not cause a substantial delay for the purposes of bringing legal proceedings, that they suspend the period for the time-barring of claims and that they do not give rise to costs — or give rise to very low costs — for the parties, and only if electronic means are not the only means by which the settlement procedure may be accessed and interim measures are possible in exceptional cases where the urgency of the situation so requires (see, to that effect, judgments of 18 March 2010,   
Alassini and Others  
, C-317/08 to C-320/08, EU:C:2010:146, paragraph 67, and of 14 June 2017,   
Menini and Rampanelli  
, C-75/16, EU:C:2017:457, paragraph 61).  
71      Those various conditions apply   
mutatis mutandis  
 to the obligation to exhaust the available administrative remedies at issue in the case in the main proceedings.  
72      It is therefore for the referring court to examine whether the practical arrangements for the exercise of administrative remedies available under Slovak law do not disproportionately affect the right to an effective remedy before a court referred to in Article 47 of the Charter.  
73      In that context, it should be noted that Mr Puškár claimed, inter alia, that there was uncertainty as to whether the period for bringing a legal action before the national court begins before a decision has been taken, was taken in the context of an action brought before the administrative authority concerned. If that were the case, the obligation to exhaust available administrative remedies, which might prevent access to judicial protection, would not comply with the right to an effective remedy before a court referred to in Article 47 of the Charter.  
74      As far as delays are concerned, it should be borne in mind that Article 47(2) of the Charter provides for the right of every person to have their case dealt with within a reasonable period of time. While that right admittedly relates to judicial proceedings themselves, it may not however be undermined by a condition prior to bringing a legal action.  
75      As regards the costs which a prior administrative complaint might entail, as the Advocate General also stated in points 68 and 69 of her Opinion, although it is in principle permissible for Member States to impose an appropriate charge for bringing an action before an administrative authority, such a charge may not, however, be set at a level which might constitute an obstacle to the exercise of the right to a judicial remedy guaranteed by Article 47 of the Charter. In that regard, account must be taken of the fact that that charge adds to the costs of the judicial proceedings.  
76      In the light of all the foregoing considerations, the answer to the first question must be that Article 47 of the Charter must be interpreted as meaning that it does not preclude national legislation, which makes the exercise of a judicial remedy by a person stating that his right to protection of personal data guaranteed by Directive 95/46 has been infringed, subject to the prior exhaustion of the available administrative remedies, provided that the practical arrangements for the exercise of such remedies do not disproportionately affect the right to an effective remedy before a court referred to in that article. It is important, in particular, that the prior exhaustion of the available administrative remedies does not lead to a substantial delay in bringing a legal action, that it involves the suspension of the limitation period of the rights concerned and that it does not involve excessive costs.  
   
The third question  
77      By its third question, which it is appropriate to examine in the second place, the referring court asks, in essence, whether Article 47 of the Charter must be interpreted as precluding that a national court rejects, as evidence of an infringement of the protection of personal data conferred by Directive 95/46, a list, such as the contested list, submitted by the data subject and containing personal data relating to him, if that person had obtained that list without the consent, legally required, of the person responsible for processing that data.  
   
Admissibility  
78      Several parties and interested parties having submitted observations to the Court take the view that the third question referred for a preliminary ruling is inadmissible.  
79      First, according to Mr Puškár and the Slovak Government, that question has no connection with EU law in the absence of EU rules on the lawfulness of evidence.  
80      That argument cannot, however, be accepted.  
81      It is important to note that Mr Puškár seeks judicial review of a measure by the Slovak tax authorities, namely the drawing up of the contested list, by which the rights conferred on him by Directive 95/46 have, according to him, been infringed.  
82      The dismissal by the referring court of the evidence at issue in the main proceedings merely on the ground that Mr Puškár has obtained it without the consent, legally required, of the data controller constitutes a limitation on the right to a judicial remedy guaranteed by Article 22 of Directive 95/46 and a limitation on the right to an effective remedy before a court within the meaning of Article 47 of the Charter.  
83      On the other hand, the Czech Government has expressed doubts as to the relevance of the third question to the resolution of the dispute in the main proceedings, since one of the administrative authorities involved in that dispute, namely the Financial Administration Criminal Office, does not challenge the existence of the contested list. According to the Czech Government, the dispute in the main proceedings does not therefore raise any question as to the existence of the contested list, so that it is not necessary to decide on the admissibility of that list as evidence.  
84      In that regard, it is sufficient to note that the referring court does not appear to have decided on the circumstances surrounding the drawing up of the contested list.  
85      In those circumstances, having regard to the case-law referred to in paragraphs 49 and 50 of the present judgment, it is not clear that the interpretation sought of EU law has nothing to do with the facts or the subject matter of the dispute in the main proceedings.  
86      In the light of all the foregoing considerations, the third question must be considered to be admissible.  
   
Substance  
87      As has been stated in paragraph 82 of the present judgment, rejecting a list, such as the contested list, as evidence of an infringement of the rights conferred by Directive 95/46, constitutes a limitation on the right to an effective remedy before a court within the meaning of Article 47 of the Charter.  
88      It is clear from paragraph 62 of the present judgment that such a restriction is justified only, in accordance with Article 52(1) of the Charter, if it is provided for by law, if it respects the essence of that right and, subject to the principle of proportionality, if it is necessary and genuinely meets objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.  
89      Therefore, before the disputed list can be rejected as evidence, the referring court must first of all satisfy itself that that restriction of the right to an effective remedy is indeed provided for by national law.  
90      Next, that court must examine whether such a rejection affects the essential content of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. In that context, it will in particular be necessary to ascertain whether the existence of the contested list and the fact that it contains personal data relating to Mr Puškár are challenged in the context of the dispute in the main proceedings and, where appropriate, if he has other evidence in that regard.  
91      Finally, it will be for that court to determine whether the rejection of the contested list as evidence is necessary and does in fact satisfy the general interest objectives recognised by the European Union or the need to protect the rights and freedoms of others.  
92      In that regard, it appears that the objective of avoiding the unauthorised use of internal documents in judicial proceedings is capable of constituting a legitimate general interest objective (see, to that effect, orders of 23 October 2002,   
Austria   
v  
 Council  
, C-445/00, EU:C:2002:607, paragraph 12; of 23 March 2007,   
Stadtgemeinde Frohnleiten and Gemeindebetriebe Frohnleiten  
, C-221/06, EU:C:2007:185, paragraph 19; and of 29 January 2009,   
Donnici  
 v   
Parliament  
, C-9/08, not published, EU:C:2009:40, paragraph 13). Furthermore, where a list, such as the contested list, is intended to remain confidential and also contains personal data of other natural persons, there is a need to protect the rights of those persons.  
93      If the rejection of a list, such as the contested list, as evidence obtained without the consent, legally required, of the authority responsible for processing the data appearing on that list, appears appropriate for achieving those objectives, it is however for the referring court to ascertain whether such a rejection does not disproportionately affect the right to an effective remedy before a court referred to in Article 47 of the Charter.  
94      At the very least, if the person whose personal data is on the list enjoys a right of access to those data, such rejection appears disproportionate to those very objectives.  
95      In that regard, Article 12 of Directive 95/46 guarantees everyone a right of access to the data collected relating to him. Furthermore, it is clear from Articles 10 and 11 of Directive 95/46 that the person responsible for processing such data must provide the data subjects with certain information relating to that processing.  
96      Although Article 13(1) of Directive 95/46 limits the scope of the rights provided for in Articles 10 to 12 of that directive where such a restriction constitutes a necessary measure to safeguard, in particular, the prevention, investigation, detection and prosecution of criminal offences or an important economic or financial interest of a Member State, including taxation and monitoring, inspection or regulatory functions, it expressly requires that such restrictions are imposed by legislative measures (see, to that effect, judgment of 1 October 2015,   
Bara and Others   
v  
 Commission  
, C-201/14, EU:C:2015:638, paragraph 39).  
97      Thus, in order to assess the proportionality of a rejection of the disputed list as evidence, the referring court must examine whether its national legislation limits, in relation to the data included in the list, information and access rights laid down in Articles 10 to 12 of Directive 95/46 and if such a limitation is, where appropriate, justified. Moreover, even where that is the case and there is evidence to support a legitimate interest in the possible confidentiality of the contested list, the national courts must determine on a case-by-case basis whether this takes precedence over interest in the protection of the rights of the individual and whether, in the proceedings before that court, other means exist to ensure that confidentiality, in particular as regards the personal data of other natural persons included on that list.  
98      In the light of the foregoing considerations, the answer to the third question is that Article 47 of the Charter must be interpreted as precluding that a national court rejects, as evidence of an infringement of the protection of personal data conferred by Directive 95/46, a list, such as the contested list, submitted by the data subject and containing personal data relating to him, if that person had obtained that list without the consent, legally required, of the person responsible for processing that data, unless such rejection is laid down by national legislation and respects both the essential content of the right to an effective remedy and the principle of proportionality.  
   
The second question  
99      By its second question, the referring court asks, in essence, whether Directive 95/46 and Articles 7 and 8 of the Charter are to be interpreted as precluding the processing of personal data by the authorities of a Member State for the purpose of collecting tax and combating tax fraud such as that effected by drawing up the contested list in the main proceedings without the consent of the data subjects.  
 Admissibility  
100    According to Mr Puškár, the second question is hypothetical and of no relevance to the outcome of the dispute in the main proceedings. In his view, the national court seeks only to ascertain whether the processing of personal data by the Finance Directorate is admissible as a general rule but does not specifically address the contested list which was designed by the Finance Directorate without legal basis.  
101    It must however be taken into account, having regard to the case-law referred to in paragraphs 49 and 50 of the present judgment, and the information contained in the order for reference, that it is not clear that the interpretation of EU law sought has nothing to do with the facts or the subject matter of the dispute in the main proceedings.  
   
Substance  
102    The second question must be examined in the light of Directive 95/46, inasmuch as, as is clear inter alia from the objective of that directive, as set out in Article 1(1) thereof, as long as the conditions governing the legal processing of personal data under that directive are fulfilled, that processing shall be deemed to satisfy also the requirements laid down in Articles 7 and 8 of the Charter.  
103    As is apparent from paragraphs 33 and 34 of the present judgment, the drawing up of a list, such as the contested list, which contains the names of certain natural persons and associates them with one or more legal persons within which those natural persons purport to act as company directors, constitutes ‘processing of personal data’ within the meaning of Article 2(b) of Directive 95/46.  
104    In accordance with the provisions of Chapter II of Directive 95/46, entitled ‘General rules on the lawfulness of the processing of personal data’, subject to the exceptions permitted under Article 13 of that directive, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of that directive (see, to that effect, judgment of 1 October 2015,   
Bara and Others  
, C-201/14, EU:C:2015:638, paragraph 30).  
105    It is also important to recall that it follows from the objective of ensuring an equivalent level of protection in all Member States, pursued by that directive, that Article 7 thereof sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful (see judgment of 24 November 2011,   
ASNEF and FECEMD  
, C-468/10 and C-469/10, EU:C:2011:777, paragraph 30).  
106    In particular, it should be stated that Article 7(e) provides that personal data may lawfully be processed if ‘it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed’.  
107    The establishment of the contested list appears likely to fall within that provision.  
108    It appears that the collection of the tax and combating tax fraud, for the purposes of which the contested list is established, must be regarded as tasks carried out in the public interest within the meaning of that provision.  
109    However, it is for the referring court to determine whether the Slovak authorities having compiled the list or those to whom it was notified have been invested with those missions by Slovak legislation.  
110    In that regard, it must be observed that Article 6(1)(b) of Directive 95/46 requires that personal data be collected for specific, explicit and legitimate purposes. As the Advocate General stated in point 106 of her Opinion, the objective of the processing of personal data is inextricably linked, within the scope of Article 7(e) of Directive 95/46, to the task of the controller. Consequently, the transfer of the task to the latter must clearly include the purpose of the processing.  
111    It is also for the referring court to determine whether the establishment of the contested list is necessary for the performance of the tasks carried out in the public interest at issue in the case in the main proceedings, taking account, in particular, of the precise purpose of the establishment of the contested list, the legal effects to which the persons appearing on it and the public nature of that list are subject and whether or not that list is of a public nature.  
112    It is important, in that regard, to ensure that the principle of proportionality is respected. The protection of the fundamental right to respect for private life at the European Union level requires that derogations from the protection of personal data and its limitations be carried out within the limits of what is strictly necessary (see, to that effect, judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 96 and the case-law cited).  
113    It is thus for the national court to ascertain whether the establishment of the contested list and the inclusion of the names of the data subjects in such a register are suitable for achieving the objectives pursued by them and whether there is no other less restrictive means in order to achieve those objectives.  
114    The fact that a person is placed on the contested list is likely to infringe some of his rights. Indeed, inclusion in that list could harm his reputation and affect his relations with the tax authorities. Likewise, such inclusion could affect the presumption of innocence of that person, set out in Article 48(1) of the Charter, as well as the freedom of enterprise enshrined in Article 16 of the Charter of legal persons associated with the natural persons included in the contested list. It appears that an infringement of this kind can be proportionate only if there are sufficient grounds to suspect the person concerned of purportedly acting as a company director of the legal persons associated with him and accordingly undermines the public interest in the collection of taxes and combating tax fraud.  
115    Although the referring court came to the conclusion that the establishment of the contested list is necessary for the performance of tasks carried out in the public interest of the controller in accordance with Article 7(e) of Directive 95/46, it should also determine that the other conditions for the lawfulness of that processing of personal data imposed by the directive are satisfied, in particular those arising under Articles 6 and 10 to 12 thereof.  
116    Furthermore, if there were grounds for limiting, under Article 13 of Directive 95/46, certain of the rights provided for in those articles, such as the right to information of the data subject, such a limitation should, as is clear from paragraph 96 of the present judgment, be necessary for the protection of an interest referred to in Article 13(1), such as, inter alia, an important economic and financial interest in the field of taxation and be based on legislative measures.  
117    In the light of the foregoing considerations, the answer to the second question is that Article 7(e) Directive 95/46 must be interpreted as not precluding the processing of personal data by the authorities of a Member State for the purpose of collecting tax and combating tax fraud such as that effected by drawing up the contested list in the main proceedings, without the consent of the data subjects, provided that, first, those authorities were invested by the national legislation with tasks carried out in the public interest within the meaning of that article, that the drawing-up of that list and the inclusion on it of the names of the data subjects in fact be appropriate and necessary for the purpose of attaining the objectives pursued and that there be sufficient indications to assume that the data subjects are rightly included in that list and, second, that all of the conditions for the lawfulness of that processing of personal data imposed by Directive 95/46 be satisfied.  
   
The fourth question  
118    By its fourth question, the national court asks, in essence, whether Article 47 of the Charter must be interpreted as precluding a national court, having found that, in a case before it, there are differences between the case-law of the European Court of Human Rights and that of the Court of Justice, following the latter.  
119    That question was raised by the referring court in general terms, without the latter clarifying in a clear and concrete manner what those differences are.  
120    It should be borne in mind that the requirements concerning the content of a request for a preliminary ruling are expressly set out in Article 94 of the Court’s Rules of Procedure, of which the national court should, in the context of the cooperation instituted by Article 267 TFEU, be aware and which it is bound to observe scrupulously. Thus, the referring court must set out the precise reasons that led it to raise the question of the interpretation of certain provisions of EU law and to consider it necessary to refer questions to the Court of Justice for a preliminary ruling. The Court has previously held that it is essential that the national court should give at the very least some explanation of the reasons for the choice of the EU law provisions which it seeks to have interpreted and of the link it establishes between those provisions and the national legislation applicable to the proceedings pending before it (judgment of 9 March 2017,   
Milkova  
, C-406/15, EU:C:2017:198, paragraphs 72 and 73 and the case-law cited).  
121    Those requirements also appear in the recommendations of the Court of Justice of the European Union to national courts and tribunals in relation to the initiation of preliminary ruling proceedings (OJ 2016 C 439, p. 1).  
122    In the present case, it must be held that the fourth question does not satisfy the requirements set out in the preceding paragraphs.  
123    It should also be borne in mind that, in accordance with the Court’s settled case-law, the justification for making a request for a preliminary ruling is not for advisory opinions to be delivered on general or hypothetical questions, but rather that it is necessary for the effective resolution of a dispute concerning EU law (see judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 130).  
124    It follows that the third question is inadmissible.  
   
Costs  
125    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
1.      Article 47 of the Charter of Fundamental Rights of the European Union must be interpreted as meaning that it does not preclude national legislation, which makes the exercise of a judicial remedy by a person stating that his right to protection of personal data guaranteed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, has been infringed, subject to the prior exhaustion of the remedies available to him before the national administrative authorities, provided that the practical arrangements for the exercise of such remedies do not disproportionately affect the right to an effective remedy before a court referred to in that article. It is important, in particular, that the prior exhaustion of the available remedies before the national administrative authorities does not lead to a substantial delay in bringing a legal action, that it involves the suspension of the limitation period of the rights concerned and that it does not involve excessive costs.  
2.      Article 47 of the Charter of Fundamental Rights of the European Union must be interpreted as precluding that a national court rejects, as evidence of an infringement of the protection of personal data conferred by Directive 95/46, a list, such as the contested list, submitted by the data subject and containing personal data relating to him, if that person had obtained that list without the consent, legally required, of the person responsible for processing that data, unless such rejection is laid down by national legislation and respects both the essential content of the right to an effective remedy and the principle of proportionality.  
3.      Article 7(e) Directive 95/46 must be interpreted as not precluding the processing of personal data by the authorities of a Member State for the purpose of collecting tax and combating tax fraud such as that effected by drawing up of a list of persons such as that at issue in the main proceedings, without the consent of the data subjects, provided that, first, those authorities were invested by the national legislation with tasks carried out in the public interest within the meaning of that article, that the drawing-up of that list and the inclusion on it of the names of the data subjects in fact be adequate and necessary for the attainment of the objectives pursued and that there be sufficient indications to assume that the data subjects are rightly included in that list and, second, that all of the conditions for the lawfulness of that processing of personal data imposed by Directive 95/46 be satisfied.

ID: 9154199d-e4ae-48d1-9b8a-8cf081e5ee7d

Judgment of 24 Nov 2011, C-468/10 (  
ASNEF  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
   
JUDGMENT OF THE COURT (Third Chamber)  
24 November 2011 (\*)  
(Processing of personal data – Directive 95/46/EC – Article 7(f) – Direct effect)  
In Joined Cases C-468/10 and C-469/10,  
REFERENCES for a preliminary ruling under Article 267 TFEU from the Tribunal Supremo (Spain), made by decisions of 15 July 2010, received at the Court on 28 September 2010, in the proceedings  
Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)  
 (C-468/10),  
Federación de Comercio Electrónico y Marketing Directo (FECEMD)   
(C-469/10)   
v  
Administración del Estado,  
intervening parties:  
Unión General de Trabajadores (UGT)  
 (C-468/10 and C-469/10),  
Telefónica de España SAU  
 (C-468/10),  
France Telecom España SA  
 (C-468/10 and C-469/10),  
Telefónica Móviles de España SAU   
(C-469/10),  
Vodafone España SA   
(C-469/10),  
Asociación de Usuarios de la Comunicación   
(C-469/10),  
THE COURT (Third Chamber),  
composed of K. Lenaerts (Rapporteur), President of the Chamber, R. Silva de Lapuerta, E. Juhász, T. von Danwitz and D. Šváby, Judges,  
Advocate General: P. Mengozzi,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 15 September 2011,  
after considering the observations submitted on behalf of:  
–        Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), by C. Alonso Martínez and A. Creus Carreras, abogados,  
–        Federación de Comercio Electrónico y Marketing Directo (FECEMD), by R. García del Poyo Vizcaya and M.Á. Serrano Pérez, abogados,  
–        the Spanish Government, by M. Muñoz Pérez, acting as Agent,  
–        the European Commission, by I. Martínez del Peral and B. Martenczuk, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        These references for a preliminary ruling concern the interpretation of Article 7(f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).   
2        The references have been made in two sets of proceedings between, on the one hand, Asociación Nacional de Establecimientos Financieros de Crédito (National Association of Credit Institutions) (‘ASNEF’), in the first case, and Federación de Comercio Electrónico y Marketing Directo (Federation of Electronic Commerce and Direct Marketing) (‘FECEMD’), in the second case, and, on the other, the Administración del Estado.  
   
Legal context  
   
European Union (‘EU’) law  
 Directive 95/46  
3        Recitals 7, 8 and 10 in the preamble to Directive 95/46 read as follows:   
‘(7)      … the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; … this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; … this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;  
(8)      …, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; … this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market …; … Community action to approximate those laws is therefore needed;  
…  
(10)      … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [signed in Rome on 4 November 1950 (‘the ECHR’)] and in the general principles of Community law; …, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community’.  
4        Article 1 of Directive 95/46, entitled ‘Object of the Directive’, is drafted in the following terms:   
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’  
5        Article 5 of Directive 95/46 is worded as follows:   
‘Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.’  
6        Article 7 of Directive 95/46 states:   
‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent; or  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
7        Article 13(1) of Directive 95/46 provides:   
‘Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
(e)      an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;  
(f)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);  
(g)      the protection of the data subject or of the rights and freedoms of others.’  
   
National law  
 Organic Law 15/1999  
8        Organic Law 15/1999 on the protection of personal data (BOE no 298 of 14 December 1999, p. 43088) transposes Directive 95/46 into Spanish law.   
9        Article 3(j) of Organic Law 15/1999 sets out ‘public sources’ in an exhaustive and restrictive list, which reads as follows:   
‘… those files that can be consulted by any person, unhindered by a limiting provision or by any requirement other than, where relevant, payment of a fee. Public sources are, exclusively, the electoral roll, telephone directories subject to the conditions laid down in the relevant regulations and lists of persons belonging to professional associations containing only data on the name, title, profession, activity, academic degree, address and an indication of membership of the association. Newspapers and official bulletins and the media are also public sources.’   
10      Article 6(1) of Organic Law 15/1999 makes the processing of data subject to the data subject’s unambiguous consent, unless otherwise provided by law. Thus, Article 6(2),   
in fine  
, of Organic Law 15/1999 provides that consent is not required, inter alia, ‘… when the data are included in public sources and their processing is necessary for the purposes of the legitimate interests pursued by the controller of the file or by the third party to whom the data are disclosed, except where this infringes the fundamental rights and freedoms of the data subject.’   
11      Article 11(1) of Organic Law 15/1999 reiterates the need for the data subject’s consent in order to disclose personal data to third parties, while Article 11(2), however, provides that that consent is not necessary, inter alia, in relation to data appearing in public sources.   
 Royal Decree 1720/2007  
12      The Spanish Government implemented Organic Law 15/1999 by way of Royal Decree 1720/2007 (BOE No 17 of 19 January 2008, p. 4103).   
13      Article 10(1) of Royal Decree 1720/2007 allows the processing and transfer of personal data in cases where the data subject has given prior consent.   
14      However, Article 10(2) of Royal Decree 1720/2007 provides:  
‘… personal data may be processed or transferred without the data subject’s consent when:   
(a)      it is authorised by a regulation having the force of law or under Community law and, in particular, when one of the following situations applies:   
–        the purpose of the processing or transfer is to satisfy a legitimate interest of the data controller or recipient guaranteed by these rules, as long as the interest or fundamental rights and liberties of the data subjects, as provided in Article 1 of Organic Law 15/1999 of 13 December, are not overriding;  
–        the processing or transfer of data is necessary in order for the data controller to fulfil a duty imposed upon him by one of those provisions;   
(b)      the data which are the subject of processing or transfer are in sources accessible to the public and the data controller, or the third party to whom data has been communicated, has a legitimate interest in their processing or knowledge, as long as the fundamental rights and liberties of the data subject are not breached.   
The aforesaid notwithstanding, the public administration may communicate the data collected from sources accessible to the public to the data controllers of privately owned files pursuant to this subsection only when they are so authorised by a regulation having the force of law.’   
   
The disputes in the main proceedings and the questions referred for a preliminary ruling  
15      ASNEF, on the one hand, and FECEMD, on the other hand, have brought administrative proceedings challenging several articles of Royal Decree 1720/2007.   
16      Among the contested provisions are the first indent of Article 10(2)(a) and the first subparagraph of Article 10(2)(b) of Royal Decree 1720/2007, which ASNEF and FECEMD believe are in breach of Article 7(f) of Directive 95/46.   
17      In particular, ASNEF and FECEMD take the view that Spanish law adds, to the condition relating to the legitimate interest in data processing without the data subject’s consent, a condition, which does not exist in Directive 95/46, to the effect that the data should appear in public sources.   
18      The Tribunal Supremo (Supreme Court, Spain) considers that the merits of the actions brought by ASNEF and FECEMD respectively depend to a large extent on the interpretation by the Court of Article 7(f) of Directive 95/46. Accordingly, it states that, if the Court were to hold that Member States are not entitled to add extra conditions to those required by that provision, and if that provision were to be found to have direct effect, Article 10(2)(b) of Royal Decree 1720/2007 would have to be set aside.   
19      The Tribunal Supremo explains that, in the absence of the data subject’s consent, and in order to allow processing of that data subject’s personal data that is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, Spanish law requires not only that the fundamental rights and freedoms of the data subject be respected, but also that the data appear in the files listed in Article 3(j) of Organic Law 15/1999. In that regard, it takes the view that Organic Law 15/1999 and Royal Decree 1720/2007 restrict the scope of Article 7(f) of Directive 95/46.   
20      In the view of the Tribunal Supremo, that restriction constitutes a barrier to the free movement of personal data that is compatible with Directive 95/46 only if the interest or the fundamental rights and freedoms of the data subject so require. It concludes that the only way to avoid a contradiction between Directive 95/46 and Spanish law is to hold that the free movement of personal data appearing in files other than those listed in Article 3(j) of Organic Law 15/1999 infringes the interest or the fundamental rights and freedoms of the data subject.   
21      However, the Tribunal Supremo is unsure whether such an interpretation is in accordance with the intention of the EU legislature.   
22      In those circumstances, being of the view that the outcome of both the cases before it depends on the interpretation of provisions of EU law, the Tribunal Supremo decided to stay the proceedings and to refer the following questions, which are formulated in identical terms in both cases, to the Court for a preliminary ruling:   
‘(1)      Must Article 7(f) of [Directive 95/46] be interpreted as precluding the application of national rules which, in the absence of the interested party’s consent, and to allow processing of his personal data that is necessary to pursue a legitimate interest of the controller or of third parties to whom the data will be disclosed, not only require that fundamental rights and freedoms should not be prejudiced, but also require the data to appear in public sources?  
(2)      Are the conditions for conferring on it direct effect, set out in the case-law of the Court … met by the abovementioned Article 7(f)?’   
23      By order of the President of the Court of 26 October 2010, Cases C-468/10 and C-469/10 were joined for the purposes of the written and oral procedure and the judgment.  
   
Consideration of the questions referred   
   
The first question  
24      By its first question, the national court asks, in essence, whether Article 7(f) of Directive 95/46 must be interpreted as precluding national rules which, in the absence of the data subject’s consent, and in order to allow such processing of that data subject’s personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom the data are disclosed, requires not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources.  
25      Article 1 of Directive 95/46 requires Member States to ensure the protection of the fundamental rights and freedoms of natural persons, and in particular their privacy, in relation to the handling of personal data (see, to that effect, Case C-524/06   
Huber   
[2008] ECR I-9705, paragraph 47).   
26      In accordance with the provisions of Chapter II of Directive 95/46, entitled ‘General rules on the lawfulness of the processing of personal data’, all processing of personal data must, subject to the exceptions permitted under Article 13, comply, first, with the principles relating to data quality set out in Article 6 of Directive 95/46 and, secondly, with one of the six principles for making data processing legitimate listed in Article 7 of Directive 95/46 (see, to that effect, Joined Cases C-465/00, C-138/01 and C-139/01   
Österreichischer Rundfunk and Others  
 [2003] ECR I-4989, paragraph 65, and   
Huber  
, paragraph 48).   
27      According to recital 7 in the preamble to Directive 95/46, the establishment and functioning of the internal market are liable to be seriously affected by differences in national rules applicable to the processing of personal data (Case C-101/01   
Lindqvist   
[2003] ECR I-12971, paragraph 79).  
28      In that context, it must be noted that Directive 95/46 is intended, as appears from, inter alia, recital 8 in the preamble thereto, to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. Recital 10 adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the EU (see, to that effect,   
Lindqvist  
, paragraph 95, and   
Huber  
, paragraph 50).  
29      Accordingly, it has been held that the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete. It is upon that view that Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate (  
Lindqvist  
, paragraph 96).   
30      Consequently, it follows from the objective of ensuring an equivalent level of protection in all Member States that Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful.   
31      That interpretation is corroborated by the term ‘may be processed only if’ and its juxtaposition with ‘or’ contained in Article 7 of Directive 95/46, which demonstrate the exhaustive and restrictive nature of the list appearing in that article.   
32      It follows that Member States cannot add new principles relating to the lawfulness of the processing of personal data to Article 7 of Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7.   
33      The foregoing interpretation is not brought into question by Article 5 of Directive 95/46. Article 5 merely authorises Member States to specify, within the limits of Chapter II of that directive and, accordingly, Article 7 thereof, the conditions under which the processing of personal data is lawful.  
34      The margin of discretion which Member States have pursuant to Article 5 can therefore be used only in accordance with the objective pursued by Directive 95/46 of maintaining a balance between the free movement of personal data and the protection of private life (  
Lindqvist  
, paragraph 97).   
35      Directive 95/46 includes rules with a degree of flexibility and, in many instances, leaves to the Member States the task of deciding the details or choosing between options (  
Lindqvist  
, paragraph 83). A distinction, consequently, must be made between national measures that provide for additional requirements amending the scope of a principle referred to in Article 7 of Directive 95/46, on the one hand, and national measures which provide for a mere clarification of one of those principles, on the other hand. The first type of national measure is precluded. It is only in the context of the second type of national measure that Member States have, pursuant to Article 5 of Directive 95/46, a margin of discretion.   
36      It follows that, under Article 5 of Directive 95/46, Member States also cannot introduce principles relating to the lawfulness of the processing of personal data other than those listed in Article 7 thereof, nor can they amend, by additional requirements, the scope of the six principles provided for in Article 7.   
37      In the present cases, Article 7(f) of Directive 95/46 provides that the processing of personal data is lawful if it is ‘necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)’.  
38      Article 7(f) sets out two cumulative conditions that must be fulfilled in order for the processing of personal data to be lawful: firstly, the processing of the personal data must be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed; and, secondly, such interests must not be overridden by the fundamental rights and freedoms of the data subject.   
39      It follows that, in relation to the processing of personal data, Article 7(f) of Directive 95/46 precludes any national rules which, in the absence of the data subject’s consent, impose requirements that are additional to the two cumulative conditions set out in the preceding paragraph.   
40      However, account must be taken of the fact that the second of those conditions necessitates a balancing of the opposing rights and interests concerned which depends, in principle, on the individual circumstances of the particular case in question and in the context of which the person or the institution which carries out the balancing must take account of the significance of the data subject’s rights arising from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’).   
41      In this regard, it must be noted that Article 8(1) of the Charter states that ‘[e]veryone has the right to the protection of personal data concerning him or her’. That fundamental right is closely connected with the right to respect for private life expressed in Article 7 of the Charter (Joined Cases C-92/09 and C-93/09   
Volker und Markus Schecke and Eifert   
[2010] ECR I-0000, paragraph 47).  
42      According to the Court’s case-law, the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (  
Volker und Markus Schecke and Eifert  
, paragraph 52). However, it follows from Articles 8(2) and 52(1) of the Charter that, under certain conditions, limitations may be imposed on that right.   
43      Moreover, Member States must, when transposing Directive 95/46, take care to rely on an interpretation of that directive which allows a fair balance to be struck between the various fundamental rights and freedoms protected by the EU legal order (see, by analogy, Case C-275/06   
Promusicae  
 [2008] ECR I-271, paragraph 68).   
44      In relation to the balancing which is necessary pursuant to Article 7(f) of Directive 95/46, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject’s fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources.  
45      Unlike the processing of data appearing in public sources, the processing of data appearing in non-public sources necessarily implies that information relating to the data subject’s private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed. This more serious infringement of the data subject’s rights enshrined in Articles 7 and 8 of the Charter must be properly taken into account by being balanced against the legitimate interest pursued by the data controller or by the third party or parties to whom the data are disclosed.   
46      In that regard, it must be noted that there is nothing to preclude Member States, in the exercise of their discretion laid down in Article 5 of Directive 95/46, from establishing guidelines in respect of that balancing.   
47      However, it is no longer a precision within the meaning of Article 5 of Directive 95/46 if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing, for those categories, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case.   
48      Consequently, without prejudice to Article 8 of Directive 95/46 concerning the processing of particular categories of data, a provision which is not at issue in the main proceedings, Article 7(f) of that directive precludes a Member State from excluding, in a categorical and generalised manner, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in a particular case.   
49      In light of those considerations, the answer to the first question is that Article 7(f) of Directive 95/46 must be interpreted as precluding national rules which, in the absence of the data subject’s consent, and in order to allow such processing of that data subject’s personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that those data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.  
   
The second question  
50      By its second question, the national court asks, in essence, whether Article 7(f) of Directive 95/46 has direct effect.  
51      In that regard, it must be recalled that, according to settled case-law of the Court, whenever the provisions of a directive appear, so far as their subject-matter is concerned, to be unconditional and sufficiently precise, they may be relied on before the national courts by individuals against the State where the latter has failed to implement that directive in domestic law by the end of the period prescribed or where it has failed to implement that directive correctly (see Case C-203/10   
Auto Nikolovi   
[2011] ECR I-0000, paragraph 61 and the case-law cited).   
52      It must be stated that Article 7(f) of Directive 95/46 is a provision that is sufficiently precise to be relied on by an individual and applied by the national courts. Moreover, while that directive undoubtedly confers on the Member States a greater or lesser discretion in the implementation of some of its provisions, Article 7(f), for its part, states an unconditional obligation (see, by analogy,   
Österreichischer Rundfunk and Others  
, paragraph 100).  
53      The use of the expression ‘except where’ in the actual text of Article 7(f) of Directive 95/46 is not such, by itself, as to cast doubt on the unconditional nature of that provision, within the meaning of that case-law.  
54      That expression is intended to establish one of the two cumulative elements provided for in Article 7(f) of Directive 95/46 to which the possibility of processing personal data without the data subject’s consent is subject. As that element is defined, it does not deprive Article 7(f) of its precise and unconditional nature.  
55      The answer to the second question is therefore that Article 7(f) of Directive 95/46 has direct effect.   
   
Costs  
56      Since these proceedings are, for the parties to the main proceedings, a step in the actions pending before the national court, the decisions on costs are a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.   
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 7(f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as precluding national rules which, in the absence of the data subject’s consent, and in order to allow such processing of that data subject’s personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.  
2.        
Article 7(f) of Directive 95/46 has direct effect.

ID: 947f9d32-cc95-4f23-9990-343b96073599

of 5 Dec 2023, C-807/21 (  
Deutsche Wohnen  
)  
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Powers   
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Administrative fines   
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Administrative fines   
   
JUDGMENT OF THE COURT (Grand Chamber)  
5 December 2023 (\*)  
(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 4(7) – Concept of ‘controller’ – Article 58(2) – Powers of supervisory authorities to apply corrective powers – Article 83 – Imposition of administrative fines on a legal person – Conditions – Discretion of the Member States – Requirement that the infringement be intentional or negligent)  
In Case C-807/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Kammergericht Berlin (Higher Regional Court, Berlin, Germany), made by decision of 6 December 2021, received at the Court on 21 December 2021, in the proceedings  
Deutsche Wohnen SE  
v  
Staatsanwaltschaft Berlin,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, C. Lycourgos, E. Regan, T. von Danwitz, Z. Csehi, O. Spineanu–Matei, Presidents of Chambers, M. Ilešič, J.-C. Bonichot, L.S. Rossi, A. Kumin, N. Jääskinen (Rapporteur), N. Wahl and M. Gavalec, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 17 January 2023,  
after considering the observations submitted on behalf of:  
–        Deutsche Wohnen SE, by O. Geiss, K. Mertens, N. Venn and T. Wybitul, Rechtsanwälte,  
–        the German Government, by J. Möller and P.-L. Krüger, acting as Agents,  
–        the Estonian Government, by M. Kriisa, acting as Agent,  
–        the Netherlands Government, by C.S. Schillemans, acting as Agent,  
–        the Norwegian Government, by L.-M. Moen Jünge, M. Munthe-Kaas and T. Westhagen Edell, acting as Agents,  
–        the European Parliament, by G.C. Bartram and P. López-Carceller, acting as Agents,   
–        the Council of the European Union, by J. Bauerschmidt and K. Pleśniak, acting as Agents,  
–        the European Commission, by A. Bouchagiar, F. Erlbacher, H. Kranenborg and G. Meessen, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 27 April 2023,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 83(4) to (6) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (‘the GDPR’).  
2        The request has been made in proceedings between Deutsche Wohnen SE (‘DW’) and the Staatsanwaltschaft Berlin (Berlin Public Prosecutor’s Office, Germany) concerning an administrative fine imposed on DW pursuant to Article 83 of the GDPR in respect of an infringement of Article 5(1)(a), (c) and (e), Article 6 and Article 25(1) of that regulation.  
   
Legal context  
   
European Union law  
3        Recitals 9, 10, 11,13, 74, 129 and 150 of the GDPR state:  
‘(9)      … Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. …  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. … This Regulation also provides a margin of manoeuvre for Member States to specify [their] rules, including for the processing of special categories of personal data … To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.  
(11)      Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.  
…  
(13)      In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. …  
…  
(74)      The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.  
…  
(129)      In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions … In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. …  
…  
(150)      In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. …’  
4        Article 4 of that regulation provides as follows:  
‘For the purposes of this Regulation:  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;  
(8)      “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;  
…  
(18)      “enterprise” means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;  
…’  
5        Article 58 of that regulation, entitled ‘Powers’, provides, in paragraphs 2 and 4:  
‘2.      Each supervisory authority shall have all of the following corrective powers:   
(a)      to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;  
(b)      to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;  
…  
(d)      to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;  
…  
(f)      to impose a temporary or definitive limitation including a ban on processing;  
…  
(i)      to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;  
…  
4.      The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the [Charter of Fundamental Rights of the European Union].’  
6        Article 83 of that regulation, entitled ‘General conditions for imposing administrative fines’, provides:  
‘1.      Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.  
2.      Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:  
(a)      the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;   
(b)      the intentional or negligent character of the infringement;  
(c)      any action taken by the controller or processor to mitigate the damage suffered by data subjects;  
(d)      the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;  
(e)      any relevant previous infringements by the controller or processor;  
(f)      the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;  
(g)      the categories of personal data affected by the infringement;  
(h)      the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;  
(i)      where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject matter, compliance with those measures;  
(j)      adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and  
(k)      any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.  
3.      If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.  
4.      Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to [EUR 10 000 000], or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:  
(a)      the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;  
…  
5.      Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to [EUR 20 000 000], or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:  
(a)      the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;  
(b)      the data subjects’ rights pursuant to Articles 12 to 22;  
…  
(d)      any obligations pursuant to Member State law adopted under Chapter IX;  
(e)      non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).  
6.      Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to [EUR 20 000 000], or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.  
7.      Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.  
8.      The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.  
…’  
   
German law  
7        The first sentence of Paragraph 41(1) of the Bundesdatenschutzgesetz (Federal Law on data protection) of 30 June 2017 (BGBl. 2017 I, p. 2097), provides that, unless otherwise provided for in that law, the provisions of the Gesetz über Ordnungswidrigkeiten (Law on administrative offences) of 24 May 1968 (BGBl. 1968 I, p. 481) in the version in the Communication of 19 February 1987 (BGBl. 1987 I, p. 602), as amended by the Law of 19 June 2020 (BGBl. 2020 I, p. 1350; ‘the OWiG’), are applicable to the infringements referred to in Article 83(4) to (6) of the GDPR.  
8        Paragraph 30 of the OWiG, entitled ‘Fines imposed on legal persons and associations of persons’, provides:  
‘(1)      Where a person acting  
1.      as a body authorised to represent a legal person or as a member of such a body,  
2.      as chairperson of an association which does not have legal capacity or as a member of its executive board,  
3.      as a partner authorised to represent a partnership having legal capacity,  
4.      as Generalbevollmächtigte (holder of a commercial power of attorney) or in the performance of a management function as Prokurist (holder of a general commercial power of attorney) or as Handlungsbevollmächtigte (person authorised to conduct certain commercial transactions) of a legal person or of an association of persons referred to in points 2 or 3 above, or  
5.      As a person otherwise responsible for the management of the business or undertaking of a legal person or of an association of persons referred to in points 2 or 3 above, which includes supervision of the management of the business or any other exercise of supervisory powers in a senior function,  
has committed a criminal or administrative offence, as a result of which the obligations incumbent on the legal person or association of persons have been contravened or that legal person or association of persons has been enriched or was intended to be enriched, a fine may be imposed on such legal person or association of persons.  
…  
(4)      If criminal proceedings or administrative proceedings involving the imposition of fines are not initiated in respect of the criminal offence or administrative offence, or if such proceedings are discontinued, or if a penalty is not sought, the fine may be determined independently. Statutory provision may also be made to the effect that a fine may be determined independently in further cases. However, a fine shall not be determined independently in respect of the legal person or association of persons where the criminal or administrative offence cannot for any legal reason be penalised …’  
9        Paragraph 130 of the OWiG provides:  
‘1.      A person who, as owner of a business or undertaking, intentionally or negligently fails to take the necessary supervisory measures to prevent, within the business or undertaking, breach of the obligations to which the owner is subject and infringement of which is punishable by a criminal penalty or a fine, shall be deemed to have committed an administrative offence if such breach could have been prevented or made more difficult by means of appropriate supervision. The necessary supervisory measures shall also include the appointment, careful selection and monitoring of the persons responsible for supervision.  
…  
(3)      Where the breach of an obligation is punishable by a criminal penalty, the administrative offence may be punished by a fine of up to EUR 1 million. The third sentence of Paragraph 30(2) shall apply. Where the breach of the obligation is punishable by a fine, the maximum amount of the fine imposed for the breach of the obligation to supervise shall be determined by reference to the maximum amount of the fine incurred for that breach. …’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
10      DW is a listed real estate company, constituted in the legal form of a European company, with its registered office in Berlin (Germany). It holds, indirectly via participating interests in various companies, approximately 163 000 housing units and 3 000 commercial units.  
11      The owners of those units are subsidiaries of DW (‘holding companies’) which carry on the operational side of the business, while DW is responsible for the central management of the group of which it forms part, together with, inter alia, those subsidiaries. The holding companies lease the housing and commercial units which are managed by other companies in the group, known as ‘service companies’.  
12      As part of their business activities, DW and the group companies which it manages process personal data of tenants of the commercial and housing units, such as, for example, proof of identity, tax, social security and health insurance data of those tenants, as well as data relating to previous tenancies.  
13      On 23 June 2017, the Berliner Beauftragte für den Datenschutz (Berlin Data Protection Authority, Germany; ‘the supervisory authority’) informed DW during an on-the-spot inspection that companies within its group were storing the personal data of tenants in an electronic filing system in respect of which it could not be ascertained whether storage was necessary or whether there were safeguards to ensure the erasure of data which were no longer required.   
14      The supervisory authority requested DW to erase those documents from its electronic filing system by the end of 2017 at the latest. In response to that request, DW stated that it was not possible for technical and legal reasons to erase those documents.  
15      Following exchanges between DW and the supervisory authority concerning whether it was possible to erase the documents at issue, DW informed that authority that it intended to introduce a new storage system to replace the system which contained those documents.  
16      On 5 March 2019, the supervisory authority carried out an inspection at the corporate headquarters of the group managed by DW. During that inspection, DW informed that authority that the electronic filing system in question had already been decommissioned and that the data would be migrated to the new storage system imminently.  
17      By decision of 30 October 2019, the supervisory authority imposed on DW an administrative fine of EUR 14 385 000 for intentional infringement of Article 5(1)(a), (c) and (e) and of Article 25(1) of the GDPR (‘the decision at issue’). By that decision, that authority also imposed 15 other fines on DW of between EUR 3 000 and EUR 17 000 in respect of the infringement of Article 6(1) of the GDPR.  
18      In the decision at issue, the supervisory authority found, more specifically, that DW had intentionally failed, between 25 May 2018 and 5 March 2019, to take the measures necessary to allow personal data relating to tenants regularly to be erased where such data were no longer necessary or had, for some other reason, erroneously been stored. It also stated that DW had continued to store the personal data of at least 15 named tenants where such storage was not necessary.  
19      DW brought an action against that decision before the Landgericht Berlin (Regional Court, Berlin, Germany). That court closed the proceedings without taking further action, holding that the decision at issue was vitiated by such serious defects that it could not serve as a basis for the imposition of a fine.   
20      That court stated, inter alia, that the imposition of a fine on a legal person is exhaustively regulated by Paragraph 30 of the OWiG which, pursuant to Paragraph 41(1) of the Federal Law on data protection, applies to the infringements referred to in Article 83(4) to (6) of the GDPR. Under Paragraph 30 of the OWiG, a finding of an administrative infringement can be made only against a natural person and not against a legal person. In addition, only the actions of representatives of the legal person or of members of bodies thereof can be attributed to that legal person. While Paragraph 30(4) of the OWiG makes it possible, subject to certain conditions, to initiate independent proceedings for an administrative fine against a legal person, the fact remains that, also in those circumstances, it is necessary that a finding of an administrative infringement can be made against the members of bodies or representatives of the legal person concerned.  
21      The Staatsanwaltschaft Berlin (Berlin Public Prosecutor’s Office) brought an appeal against the first-instance decision before the Kammergericht Berlin (Higher Regional Court, Berlin, Germany), which is the referring court.  
22      The referring court asks, in the first place, whether, pursuant to Article 83 of the GDPR, it must be possible to impose an administrative fine on a legal person without the infringement of that regulation first being attributed to an identified natural person. In that context, the referring court considers, in particular, the relevance of the concept of an ‘undertaking’ within the meaning of Articles 101 and 102 TFEU.  
23      In that regard, the referring court explains that, according to national case-law, the limited liability regime of legal persons under national law conflicts with the regime of direct liability of undertakings laid down in Article 83 of the GDPR. According to that case-law, it is apparent, in particular, from the wording of Article 83 of the GDPR, which, in accordance with the principle of primacy of EU law, prevails over the national regime, that administrative fines may be imposed on undertakings. It is therefore not necessary for the imposition of such fines to be linked to a wrongful act on the part of the bodies or directors of legal persons, contrary to the requirements of the applicable national law.  
24      According to the referring court, that case-law, like the majority of national academic legal literature, attaches particular importance to the concept of an ‘undertaking’, within the meaning of Articles 101 and 102 TFEU, and therefore to the idea that liability is attributed to the economic entity within which the undesirable conduct, for example anticompetitive conduct, occurred. Under that ‘functional’ interpretation, all acts of all employees authorised to act on behalf of an undertaking are attributable to the undertaking, including in relation to administrative proceedings.  
25      In the second place, were the Court to find that an administrative fine must be able to be imposed directly on a legal person, the referring court raises the question of the criteria which must be applied in order to establish the liability of a legal person, as an undertaking, for an infringement of the GDPR. It wishes to ascertain, in particular, whether an administrative fine may be imposed pursuant to Article 83 of that regulation on a legal person without it being established that the infringement of that regulation attributed to that legal person was committed wrongfully.  
26      In those circumstances, the Kammergericht Berlin (Higher Regional Court, Berlin) decided to stay proceedings and to refer the following questions to the Court of Justice for preliminary ruling:  
‘(1)      Is Article 83(4) to (6) of the GDPR to be interpreted as incorporating into national law the functional concept of an undertaking and the principle of an economic entity, as defined in Articles 101 and 102 TFEU, as a result of which, by broadening the principle of a legal entity underpinning Paragraph 30 of the [OWiG], proceedings for an administrative fine may be brought against an undertaking directly and a fine imposed without requiring a finding that a natural and identified person committed an administrative offence, if necessary, in satisfaction of the objective and subjective elements of tortious liability?  
(2)      If Question 1 is answered in the affirmative: is Article 83(4) to (6) of the GDPR to be interpreted as meaning that the undertaking must have intentionally or negligently committed the breach of an obligation vicariously through an employee (see Article 23 of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (OJ 2003 L 1, p. 1)) or, is the objective fact of breach caused by it sufficient, in principle, for a fine to be imposed on that undertaking (“strict liability”)?’  
   
The request to have the written procedure reopened  
27      Following the hearing held on 17 January 2023, DW, by a document lodged at the Court Registry on 23 March 2023, applied for an order that the oral part of the procedure be reopened, pursuant to Article 83 of the Rules of Procedure of the Court of Justice.  
28      In support of its request, DW maintains, in essence, that the replies given by the referring court to the request for clarification addressed to it under Article 101 of the Rules of Procedure provide the Court with incorrect information concerning the applicable provisions of national law. A comprehensive debate concerning that issue was not possible at the hearing on 17 January 2023 because the parties had become aware of those replies only three working days before that hearing. Such a time period did not have allow for thorough preparation for the hearing.  
29      It is true that, in accordance with Article 83 of the Rules of Procedure, the Court may at any time, after hearing the Advocate General, order the reopening of the oral part of the procedure, in particular if it considers that it lacks sufficient information, or where a party has, after the close of that part of the procedure, submitted a new fact which is of such a nature as to be a decisive factor for the decision of the Court, or where the case must be decided on the basis of an argument which has not been debated between the interested persons.  
30      However, in the present case, the Court has all the information necessary to give a ruling and the present case does not have to be decided on the basis of arguments which have not been debated by the interested persons. In addition, the request that the oral part of the procedure be reopened does not disclose any new fact which is of such a nature as to be capable of being a decisive factor for the decision which the Court is called upon to make in that case.  
31      In those circumstances, the Court considers, after hearing the Advocate General, that there is no need to order that the oral part of the procedure be reopened.  
   
Consideration of the questions referred  
   
The first question  
32      By its first question, the referring court asks, in essence, whether Article 58(2) and Article 83(1) to (6) of the GDPR must be interpreted as precluding national legislation under which an administrative fine may be imposed on a legal person in its capacity as controller in respect of an infringement referred to in Article 83(4) to (6) only in so far as that infringement has previously been attributed to an identified natural person.  
33      As a preliminary point, it should be noted that, in its written observations, the German Government expressed doubts as to that interpretation of national law by the referring court, on the ground that Paragraph 130 of the OWiG also allows a fine to be imposed on a legal person outside the cases covered by Paragraph 30 of the OWiG. Furthermore, those two provisions make it possible to impose an ‘anonymous’ fine in the context of proceedings brought against the undertaking, without it being necessary to identify the natural person who committed the infringement in question.  
34      In response to a request for clarification sent to the referring court, referred to in paragraph 28 of the present judgment, that court stated that Paragraph 130 of the OWiG has no bearing on the first question referred.  
35      According to the referring court, that provision concerns the owner of a business or of an undertaking, who must have wrongfully failed to fulfil an obligation to supervise. Evidence of such a failure to fulfil obligations attributable to the owner of the undertaking is, however, extremely complex and often impossible to adduce, and the question whether a group of undertakings may be classified as an ‘undertaking’ or ‘owner of undertakings’ in accordance with that provision is the subject of divergent opinions at national level. In any event, the first question referred for a preliminary ruling is also relevant in that context.  
36      It should be recalled that, as far as the interpretation of provisions of national law is concerned, the Court is in principle required to rely on the description given in the order for reference. According to settled case-law, the Court does not have jurisdiction to interpret the internal law of a Member State (judgment of 26 January 2021,   
Hessischer Rundfunk  
, C-422/19 and C-423/19, EU:C:2021:63, paragraph 31 and the case-law cited).  
37      Consequently, the answer to the first question referred for a preliminary ruling takes as a premiss that, under the applicable national law, an administrative fine may be imposed on a legal person in its capacity as controller in respect of an infringement referred to in Article 83(4) to (6) of the GDPR only subject to the conditions laid down in Paragraph 30 of the OWiG, as set out by the referring court.  
38      In order to answer the first question referred for a preliminary ruling, it must be stated, first of all, that the principles, prohibitions and obligations laid down by the GDPR are directed, in particular, at ‘controllers’ whose responsibility extends, as stated in recital 74 of the GDPR, to any processing of personal data which they carry out themselves or which is carried out on their behalf, and who are required, on that basis, not only to implement appropriate and effective measures, but also to be able to demonstrate the compliance of processing activities with the GDPR, including the effectiveness of the measures adopted to ensure such compliance. It is that responsibility which forms, in the event of one of the infringements referred to in Article 83(4) to (6) of that regulation, the basis for the imposition of an administrative fine on the controller pursuant to Article 83 of that regulation.  
39      Article 4(7) of the GDPR defines the concept of ‘controller’ broadly, as referring to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.  
40      The objective of that broad definition in Article 4(7) of the GDPR – which expressly includes legal persons – is, in a manner consistent with the objective of the GDPR, to ensure effective protection of the fundamental rights and freedoms of natural persons and, in particular, to ensure a high level of protection of the right of every person to the protection of personal data concerning him or her (see, to that effect, judgments of 29 July 2019,   
Fashion ID  
, C-40/17, EU:C:2019:629, paragraph 66, and of 28 April 2022,   
Meta Platforms Ireland  
, C-319/20, EU:C:2022:322, paragraph 73 and the case-law cited).  
41      Furthermore, the Court has previously held that a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller (see, to that effect, judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 68).  
42      It therefore follows from the wording and purpose of Article 4(7) of the GDPR that the EU legislature did not distinguish, for the purposes of determining liability under that regulation, between natural persons and legal persons, that liability being subject to the sole condition that those persons, alone or jointly with others, determine the purposes and means of processing of personal data.  
43      Consequently, subject to what is provided for in Article 83(7) of the GDPR concerning public authorities and bodies, any person meeting that condition – regardless of whether a natural person, a legal person, a public authority, a service or another body – is responsible, inter alia, for any infringement referred to in Article 83(4) to (6) which is committed by that person or on behalf of that person.  
44      As regards legal persons, that implies, first, as the Advocate General observed, in essence, in points 57 to 59 of his Opinion, that legal persons are liable not only for infringements committed by their representatives, directors or managers, but also by any other person acting in the course of the business of those legal persons and on their behalf. Second, the administrative fines provided for in Article 83 of the GDPR in respect of such infringements must be capable of being imposed directly on legal persons where they may be classified as the controllers in question.  
45      Next, it must be stated that Article 58(2) of the GDPR sets out in detail the supervisory authorities’ corrective powers, without referring to the law of the Member States or leaving any discretion to those States. First, those powers, which include, under Article 58(2)(i) of the GDPR, the power to impose an administrative fine, relate to the controller and, second, such a controller may, as is apparent from paragraph 39 of the present judgment, be a natural person or a legal person. The substantive conditions which a supervisory authority must satisfy when imposing such a fine are, for their part, laid down in Article 83(1) to (6), in precise terms and without leaving any discretion to the Member States.  
46      It thus follows from a combined reading of Article 4(7), Article 83 and Article 58(2)(i) of the GDPR that an administrative fine in respect of an infringement referred to in Article 83(4) to (6) may also be imposed on legal persons where they are controllers. By contrast, no provision of the GDPR permits the inference that the imposition of an administrative fine on a legal person as a controller is subject to a previous finding that that infringement was committed by an identified natural person.  
47      It is true that it is apparent from Article 58(4) and Article 83(8) of the GDPR, read in the light of recital 129 of that regulation, that the exercise by the supervisory authority of its powers under those articles is to be subject to appropriate procedural safeguards in accordance with EU and Member State law, including effective judicial remedy and due process.  
48      However, the fact that that regulation accordingly provides Member States with the possibility to lay down requirements concerning the procedure to be followed by the supervisory authorities in order to impose an administrative fine in no way means that they are also authorised to lay down, in addition to such procedural requirements, substantive conditions over and above those set by Article 83(1) to (6). In addition, the fact that the EU legislature took care to make express provision for that possibility but not the possibility to lay down such additional substantive conditions confirms that it did not provide the Member States with a margin of discretion in that regard. Those substantive conditions therefore fall solely within the scope of EU law.  
49      The literal interpretation of Article 58(2) and Article 83(1) to (6) of the GDPR set out above is borne out by the purpose of that regulation.  
50      It is apparent, in particular, from recital 10 of the GDPR that the objectives of the provisions of that regulation are, inter alia, to ensure a consistent and high level of protection of natural persons with regard to the processing of personal data within the European Union and, to that end, to ensure consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of those persons with regard to the processing of personal data throughout the European Union. Recitals 11 and 129 of the GDPR emphasise, moreover, the need to ensure, in order to ensure consistent application of that regulation, that supervisory authorities have equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and that they can impose equivalent sanctions where that regulation is infringed.  
51      To allow Member States to make it a requirement, unilaterally and as a necessary condition for the imposition of an administrative fine pursuant to Article 83 of the GDPR on a controller who is a legal person, that the infringement in question is first attributed or attributable to an identified natural person, would be contrary to that purpose of the GDPR. In addition, such an additional requirement would, ultimately, risk weakening the effectiveness and deterrent effect of administrative fines imposed on legal persons as controllers, contrary to Article 83(1) of the GDPR.  
52      In that regard, it should be recalled that the second paragraph of Article 288 TFEU provides that an EU regulation is to be binding in its entirety and directly applicable in all Member States, which precludes, unless otherwise provided, Member States from taking steps which are intended to alter the scope of such a regulation. In addition, the Member States are under a duty, by virtue of the obligations arising from the FEU Treaty, not to obstruct the direct applicability inherent in regulations. In particular, they must not adopt a measure by which the nature of EU law and the consequences which arise from it are concealed from the persons concerned (judgment of 15 November 2012,   
Al-Aqsa  
 v   
Council   
and   
Netherlands  
 v   
Al-Aqsa  
, C-539/10 P and C-550/10 P, EU:C:2012:711, paragraphs 86 and 87 and the case-law cited).  
53      Lastly, in view of the referring court’s questions, it should be stated that the concept of an ‘undertaking’, within the meaning of Articles 101 and 102 TFEU, has no bearing on whether and under what conditions an administrative fine may be imposed pursuant to Article 83 of the GDPR on a controller who is a legal person, since that question is exhaustively regulated by Article 58(2) and Article 83(1) to (6) of that regulation.  
54      That concept is relevant only for the purpose of determining the amount of the administrative fine imposed under Article 83(4) to (6) of the GDPR on a controller.  
55      As the Advocate General observed in point 45 of his Opinion, the reference in recital 150 of the GDPR to the concept of an ‘undertaking’, within the meaning of Articles 101 and 102 TFEU, is to be understood in that specific context of the calculation of administrative fines imposed in respect of the infringements referred to in Article 83(4) to (6) of the GDPR.  
56      In that regard, it should be stated that, for the purposes of applying the competition rules, referred to in Articles 101 and 102 TFEU, that concept covers any entity engaged in an economic activity, irrespective of the legal status of that entity and the way in which it is financed. The concept of an undertaking therefore defines an economic unit even if in law that economic unit consists of several persons, natural or legal. That economic unit consists of a unitary organisation of personal, tangible and intangible elements which pursues a specific economic aim on a long-term basis (judgment of 6 October 2021,   
Sumal  
, C-882/19, EU:C:2021:800, paragraph 41 and the case-law cited).  
57      Accordingly, it is apparent from Article 83(4) to (6) of the GDPR, which concerns the calculation of administrative fines in respect of the infringements listed in those paragraphs, that, where the addressee of the administrative fine is or forms part of an undertaking, within the meaning of Articles 101 and 102 TFEU, the maximum amount of the administrative fine is calculated on the basis of a percentage of the total worldwide annual turnover in the preceding business year of the undertaking concerned.  
58      In short, as the Advocate General observed in point 47 of his Opinion, only an administrative fine determined on the basis of the actual or material economic capacity of the person on which it is imposed, and therefore imposed by the supervisory authority, relying, as regards the amount of that fine, on the concept of an economic unit within the meaning of the case-law cited in paragraph 56 of the present judgment, is capable of satisfying the three conditions set out in Article 83(1) of the GDPR, namely to be effective, proportionate and dissuasive.  
59      Therefore, where a supervisory authority decides, by virtue of its powers under Article 58(2) of the GDPR, to impose on a controller, which is or forms part of an undertaking, within the meaning of Articles 101 and 102 TFEU, an administrative fine pursuant to Article 83 of that regulation, that authority is required to take as its basis, under Article 83 GDPR, read in the light of recital 150 of that regulation, when calculating administrative fines in respect of the infringements referred to in Article 83(4) to (6) of the GDPR, the concept of an ‘undertaking’, within the meaning of Articles 101 and 102 TFEU.  
60      In the light of the foregoing, the answer to the first question must be that Article 58(2)(i) and Article 83(1) to (6) of the GDPR must be interpreted as precluding national legislation under which an administrative fine may be imposed on a legal person in its capacity as controller in respect of an infringement referred to in Article 83(4) to (6) only in so far as that infringement has previously been attributed to an identified natural person.  
   
The second question   
61      By its second question, which is asked in the event that the first question is answered in the affirmative, the referring court asks, in essence, whether Article 83 of the GDPR must be interpreted as meaning that an administrative fine may be imposed pursuant to that provision only where it is established that the controller, which is both a legal person and an undertaking, intentionally or negligently committed an infringement referred to in Article 83(4) to (6) of the GDPR.  
62      In that regard, it should be recalled that it is apparent from Article 83(1) of the GDPR that administrative fines must be effective, proportionate and dissuasive. However, Article 83 of the GDPR does not expressly state that the infringements referred to in Article 83(4) to (6) thereof may be penalised by such a fine only if they were committed intentionally or, at the very least, negligently.  
63      The German, Estonian and Norwegian Governments and the Council of the European Union infer therefrom, inter alia, that the EU legislature intended to leave a certain discretion to the Member States in the implementation of Article 83 of the GDPR, allowing them to provide for administrative fines to be imposed pursuant to that provision, as appropriate, without it being established that the infringement of the GDPR penalised by that fine was committed intentionally or negligently.  
64      An interpretation of that nature in respect of Article 83 of the GDPR cannot be accepted.  
65      In that regard, as has been observed in paragraphs 45 and 48 of the present judgment, the substantive conditions which a supervisory authority must satisfy when it imposes an administrative fine on a controller are governed solely by EU law, since those conditions are laid down, in detail and without leaving any discretion to the Member States, in Article 83(1) to (6) of the GDPR (see also judgment of 5 December 2023,   
Nacionalinis visuomenės sveikatos centras  
, C-683/21, EU:C:2023:XXX, paragraphs 64 to 70).  
66      As regards those conditions, it should be noted that Article 83(2) of the GDPR lists the factors to which the supervisory authority is to have regard when imposing an administrative fine on the controller. Those factors include, in Article 83(2)(b) thereof, ‘the intentional or negligent character of the infringement’. By contrast, none of the factors listed in Article 83(2) of the GDPR mentions any possibility that the controller will incur liability in the absence of wrongful conduct on its part.  
67      In addition, Article 83(2) of the GDPR must be read in conjunction with Article 83(3) thereof, the purpose of which is to lay down the consequences of cumulative infringements of that regulation, according to which ‘if a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement’.  
68      Accordingly, it follows from the wording of Article 83(2) of the GDPR that only infringements of the provisions of that regulation committed wrongfully by the controller, that is to say those committed intentionally or negligently, can result in a fine being imposed on the controller pursuant to that article.  
69      The general scheme and purpose of the GDPR support that reading.  
70      First, the EU legislature has laid down a system of penalties enabling the supervisory authorities to impose the penalties which are the most appropriate according to the circumstances of each case.  
71      Indeed, Article 58(2)(i) of the GDPR provides that those authorities may impose administrative fines, pursuant to Article 83 of that regulation, ‘in addition to, or instead’ of the other corrective powers listed in Article 58(2), such as warnings, reprimands or orders. Similarly, recital 148 of the GDPR states, inter alia, that the supervisory authorities, where dealing with a minor infringement or if the administrative fine likely to be imposed would constitute a disproportionate burden to a natural person, the supervisory authorities are permitted to refrain from imposing an administrative fine and, instead, to issue a reprimand.  
72      Second, as has been stated in paragraph 50 of the present judgment, the objectives of the provisions of the GDPR are, inter alia, to ensure a consistent and high level of protection of natural persons with regard to the processing of personal data within the European Union and, to that end, to ensure consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of those persons with regard to the processing of personal data throughout the European Union. In addition, in order to ensure consistent application of the GDPR, supervisory authorities must have equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data, so that they can impose equivalent sanctions where that regulation is infringed.  
73      The existence of a system of penalties making it possible to impose, where justified by the specific circumstances of each individual case, an administrative fine pursuant to Article 83 of the GDPR creates an incentive for controllers and processors to comply with that regulation. Through their deterrent effect, administrative fines contribute to strengthening the protection of natural persons with regard to the processing of personal data and therefore constitute a key element in ensuring respect for the rights of those persons, in accordance with the purpose of that regulation of ensuring a high level of protection of such persons with regard to the processing of personal data.  
74      However, the EU legislature did not find it necessary, in order to ensure such a high level of protection, to provide for administrative fines to be imposed in the absence of wrongdoing. In view of the fact that the GDPR aims for a level of protection which is both equivalent and homogeneous, and that it must, to that end, be applied consistently throughout the European Union, it would be contrary to that purpose to allow Member States to provide for such a system for the imposition of a fine under Article 83 of the GDPR. Such a freedom of choice would, additionally, be liable to distort competition between economic operators within the European Union, which would run counter to the stated objectives of the EU legislature, in particular, those in recitals 9 and 13 of that regulation.  
75      Accordingly, it must be observed that Article 83 of the GDPR does not allow an administrative fine to be imposed in respect of an infringement referred to in paragraphs 4 to 6 thereof, without it being established that that infringement was committed intentionally or negligently by the controller and that, consequently, a culpable infringement constitutes a condition for such a fine to be imposed.  
76      In that regard, it must be clarified, as regards the question whether an infringement has been committed intentionally or negligently and is, therefore, liable to be penalised by an administrative fine pursuant to Article 83 of the GDPR, that a controller can be penalised for conduct falling within the scope of the GDPR where that controller could not be unaware of the infringing nature of its conduct, whether or not it is aware that it is infringing the provisions of the GDPR (see, by analogy, judgments of 18 June 2013,   
Schenker & Co. and Others  
, C-681/11, EU:C:2013:404, paragraph 37 and the case-law cited; of 25 March 2021,   
Lundbeck  
 v   
Commission  
, C-591/16 P, EU:C:2021:243, paragraph 156; and of 25 March 2021,   
Arrow Group and Arrow Generics  
 v   
Commission  
, C-601/16 P, EU:C:2021:244, paragraph 97).  
77      Where the controller is a legal person, it should also be clarified that for Article 83 GDPR to apply, it is not necessary for there to have been action by or even knowledge on the part of the management body of that legal person (see, by analogy, judgments of 7 June 1983,   
Musique Diffusion française and Others  
 v   
Commission  
, 100/80 to 103/80, EU:C:1983:158, paragraph 97, and of 16 February 2017,   
Tudapetrol Mineralölerzeugnisse Nils Hansen  
 v   
Commission  
, C-94/15 P, EU:C:2017:124, paragraph 28 and the case-law cited).  
78      Having regard to the foregoing, the answer to the second question is that Article 83 of the GDPR must be interpreted as meaning that an administrative fine may be imposed pursuant to that provision only where it is established that the controller, which is both a legal person and an undertaking, intentionally or negligently committed an infringement referred to in Article 83(4) to (6) thereof.  
   
Costs  
79      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 58(2)(i) and Article 83(1) to (6) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)   
must be interpreted as precluding national legislation under which an administrative fine may be imposed on a legal person in its capacity as controller in respect of an infringement referred to in Article 83(4) to (6) only in so far as that infringement has previously been attributed to an identified natural person.  
2.        
Article 83 of Regulation 2016/679  
must be interpreted as meaning that an administrative fine may be imposed pursuant to that provision only where it is established that the controller, which is both a legal person and an undertaking, intentionally or negligently committed an infringement referred to in Article 83(4) to (6) thereof.

ID: 9515bbb7-7e17-4a5d-ac50-5ddcbbd865c7

Judgment of 19 Feb 2009, C-557/07 (  
LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten  
)  
E-privacy Directive   
 >   
Electronic communications   
 >   
Data retention and access of national authorities   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
   
ORDER OF THE COURT (Eighth Chamber)  
19 February 2009 (\*)  
(Article 104(3) of the Rules of Procedure – Information society – Copyright and related rights – Saving and disclosure of certain traffic data – Protecting the confidentiality of electronic communications – ‘Intermediaries’ within the meaning of Article 8(3) of Directive 2001/29/EC)  
In Case C-557/07,  
REFERENCE for a preliminary ruling under Article 234 EC, from the Oberster Gerichtshof (Austria), made by decision of 13 November 2007, received at the Court on 14 December 2007, in the proceedings  
LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH  
v  
Tele2 Telecommunication GmbH,  
THE COURT (Eighth Chamber),   
composed of T. von Danwitz, President of the Chamber, G. Arestis and J. Malenovský (Rapporteur), Judges,  
Advocate General: Y. Bot,  
Registrar: R. Grass,  
proposing to give its decision on the second question by reasoned order in accordance with the first subparagraph of Article 104(3) of the Rules of Procedure,  
having informed the referring court that the Court proposes to give its decision on the first question by reasoned order in accordance with the second subparagraph of Article 104(3) of the Rules of Procedure,  
after calling on the interested persons referred to in Article 23 of the Statute of the Court of Justice to submit their observations in that regard,  
after hearing the Advocate General,  
makes the following  
Order  
1        This reference for a preliminary ruling concerns the interpretation of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37) and Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45).  
2        The reference has been made in the context of proceedings brought by LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH (‘LSG’) against Tele2 Telecommunication GmbH (‘Tele2’) concerning Tele2’s refusal to send LSG the names and addresses of the persons for whom it provides Internet access.  
   
Legal context  
   
Community legislation  
 The provisions concerning the information society and the protection of intellectual property, particularly copyright  
–       Directive 2000/31/EC  
3        Under Article 1(1) thereof, Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) (OJ 2000 L 178, p. 1) seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.   
–       Directive 2001/29  
4        Recital 59 in the preamble to Directive 2001/29 states:  
‘In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party’s infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.’  
5        Under Article 1(1) thereof, Directive 2001/29 concerns the legal protection of copyright and related rights in the framework of the internal market, with particular emphasis on the information society.  
6        Paragraph 1 of Article 5 of Directive 2001/29, which is entitled ‘Exceptions and limitations’, provides:  
‘Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:  
(a)      a transmission in a network between third parties by an intermediary, or  
(b)      a lawful use  
of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.’  
7        Article 8 of Directive 2001/29, which is entitled ‘Sanctions and remedies’, provides:  
‘1.      Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.  
2.      Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).  
3.      Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.’  
–       Directive 2004/48  
8        Article 8 of Directive 2004/48 is worded as follows:  
‘1.      Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:  
(a)      was found in possession of the infringing goods on a commercial scale;  
(b)      was found to be using the infringing services on a commercial scale;  
(c)      was found to be providing on a commercial scale services used in infringing activities; or  
(d)      was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.  
2.      The information referred to in paragraph 1 shall, as appropriate, comprise:  
(a)      the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;  
(b)      information on the quantities produced, manufactured, delivered, received or ordered, as well as the price obtained for the goods or services in question.  
3.      Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which:  
(a)      grant the rightholder rights to receive fuller information;  
(b)      govern the use in civil or criminal proceedings of the information communicated pursuant to this Article;  
(c)      govern responsibility for misuse of the right of information; or  
(d)      afford an opportunity for refusing to provide information which would force the person referred to in paragraph 1 to admit to his own participation or that of his close relatives in an infringement of an intellectual property right; or  
(e)      govern the protection of confidentiality of information sources or the processing of personal data.’  
 The provisions concerning the protection of personal data  
–       Directive 95/46/EC  
9        Paragraph 1 of Article 13 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), which is entitled ‘Exceptions and restrictions’, provides:  
‘1.      Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
(e)      an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;  
(f)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);  
(g)      the protection of the data subject or of the rights and freedoms of others.’  
–       Directive 2002/58  
10      Article 5(1) of Directive 2002/58 provides:  
‘Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.’  
11      Article 6 of Directive 2002/58 provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
6.      Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.’  
12      Under Article 15(1) of Directive 2002/58:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’  
   
National legislation  
13      Paragraph 81 of the Austrian Federal Law on copyright in literary and artistic works and related rights (Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte), in the version published in BGBl. I, 81/2006 (‘the Austrian Federal Law on Copyright’), provides:  
‘(1)      A person who has suffered an infringement of any exclusive rights conferred by this Law, or who fears such an infringement, shall be entitled to bring proceedings for a restraining injunction. Legal proceedings may also be brought against the proprietor of a business if the infringement is committed in the course of the activities of his business by one of his employees or by a person acting under his control, or if there is a danger that such an infringement will be committed.  
1(a)      If the person who has committed such an infringement, or by whom there is a danger of such an infringement being committed, uses the services of an intermediary for that purpose, the intermediary shall also be liable to an injunction under subparagraph (1).  
…’  
14      Paragraph 87b(2) to (3) of the Austrian Federal Law on Copyright is worded as follows:  
‘(2)      A person who has suffered an infringement of any exclusive rights conferred by this Law shall be entitled to require information as regards the origin and distribution channels of infringing goods and services, to the extent that this would not be disproportionate to the gravity of the infringement and would not infringe statutory obligations of confidentiality; the obligation to disclose information is on the infringer and on any persons who in the course of business:  
1.      have been in possession of infringing goods;  
2.      have received infringing services; or  
3.      have supplied services used for the infringement.  
(2a)      So far as is necessary, the obligation under subparagraph (2) to disclose information includes:  
1.      the names and addresses of the producers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;  
2.      the quantities produced, delivered, received or ordered, as well as the price paid for the goods or services in question.  
(3)      Intermediaries within the meaning of Paragraph 81(1a) shall give the person whose rights have been infringed information as to the identity of the infringer (name and address) or the information necessary to identify the infringer, following an application in writing by the person whose rights have been infringed, such application to include sufficient reasons. The reasons given must include in particular sufficiently precise details as to the facts which give rise to a suspicion that there has been an infringement of rights. The person whose rights have been infringed shall pay the intermediary reasonable compensation for the costs incurred in the provision of that information.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
15      LSG is a collecting society. It enforces as trustee the rights of recorded music producers in their worldwide recordings and the rights of the recording artists in respect of the exploitation of those recordings in Austria. The rights concerned are, in particular, the right to reproduce and distribute the recordings and the right to make them available to the public.  
16      Tele2 is an Internet access provider which assigns to its clients Internet Protocol Addresses (‘IP addresses’), which are most often dynamic rather than static. Tele2 is able to identify individual clients on the basis of the IP address and the period or date when it was assigned.  
17      The holders of the rights defended by LSG suffer financial loss as a result of the creation of file-sharing systems which make it possible for participants to exchange copies of saved data. In order to be able to bring civil proceedings against the perpetrators, LSG applied for an order requiring Tele2 to send it the names and addresses of the persons to whom it had provided an Internet access service and whose IP addresses, together with the day and time of the connection, were known. Tele2 took the view that it was obliged to refuse that request for information. It stated that it is not an intermediary and is not authorised to save access data.  
18      By judgment of 21 June 2006, the Handelsgericht Wien (Commercial Court, Vienna) granted LSG’s application, on the view that, as an Internet access provider, Tele2 is an intermediary within the meaning of Paragraph 81(1a) of the Austrian Federal Law on Copyright and that, as such, it is required to provide the information referred to in Paragraph 87b(3) thereof.  
19      According to the order for reference, the decision at first instance was confirmed on appeal by the Oberlandesgericht Wien (Higher Regional Court, Vienna) by judgment of 12 April 2007, in respect of which an appeal on a point of law has been brought before the Oberster Gerichtshof (Austrian Supreme Court).  
20      Before the Oberster Gerichtshof, Tele2 claims, first, that it is not an intermediary within the meaning of Paragraph 81(1a) of the Austrian Federal Law on Copyright or Article 8(3) of Directive 2001/29, since, as Internet access provider, it indeed enables the user to access the Internet, but it exercises no control, whether   
de iure  
 or   
de facto  
, over the services which the user makes use of. Secondly, the tensions in the relationship between the right to information entailed by the legal protection of copyright and the limits placed by data protection laws on the saving and disclosure of personal data have been resolved, in favour of data protection, by the Community directives.   
21      The Oberster Gerichtshof is of the view that the Opinion of the Advocate General in Case C-275/06   
Promusicae  
 [2008] ECR I-271, delivered after the present order for reference, raises doubts as to whether the right to information conferred by Paragraph 87b(3) of the Austrian Federal Law on Copyright, read in conjunction with Paragraph 81(1a) thereof, is in conformity with the directives adopted in the data protection field and, in particular, with Articles 5, 6 and 15 of Directive 2002/58. The aforementioned provisions of Austrian law require private third parties to be provided with information on personal data relating to Internet traffic, thereby imposing a duty to disclose, which presupposes that the Internet traffic data have first been processed and saved.  
22      In those circumstances, the Oberster Gerichtshof decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is the term “intermediary” in Article 5(1)(a) and Article 8(3) of Directive [2001/29] to be interpreted as including an access provider who merely provides a user with access to the network by allocating him a dynamic IP address but does not himself provide him with any services such as email, FTP or file-sharing services and does not exercise any control, whether   
de iure  
 or   
de facto  
, over the services which the user makes use of?  
(2)      If the first question is answered in the affirmative:  
Is Article 8(3) of Directive [2004/48], regard being had to Article 6 and Article 15 of Directive [2002/58], to be interpreted (restrictively) as not permitting the disclosure of personal traffic data to private third parties for the purposes of civil proceedings for alleged infringements of exclusive rights protected by copyright (rights of exploitation and use)?’  
   
The questions referred for a preliminary ruling  
23      Under Article 104(3) of the Rules of Procedure – that is to say, inter alia, where the answer to a question referred to the Court for a preliminary ruling may be clearly deduced from existing case-law or where the answer to the question admits of no reasonable doubt – the Court may give its decision by reasoned order.  
   
The second question  
24      By its second question, which it is appropriate to consider first, the national court essentially asks whether Community law, in particular Article 8(3) of Directive 2004/48, read in conjunction with Articles 6 and 15 of Directive 2002/58, precludes Member States from imposing an obligation to disclose to private third parties personal data relating to Internet traffic in order to enable them to bring civil proceedings for copyright infringements.  
25      The reply to that question can be clearly inferred from the case-law of the Court.  
26      In paragraph 53 of   
Promusicae  
, the Court stated that the exceptions provided for in Article 15(1) of Directive 2002/58, which refers expressly to Article 13(1) of Directive 95/46, include measures which are necessary for the protection of the rights and freedoms of others. As it does not specify the rights and freedoms covered by that exception, Directive 2002/58 must be interpreted as reflecting the intention of the Community legislature not to exclude from its scope the protection of the right to property or situations in which authors seek to obtain that protection through civil proceedings.   
27      The Court inferred from this, in paragraphs 54 and 55 of   
Promusicae  
, that Directive 2002/58 – in particular, Article 15(1) thereof – does not preclude the Member States from imposing an obligation to disclose personal data in the context of civil proceedings, nor does it oblige them to impose such an obligation.  
28      Moreover, the Court pointed out that the freedom which Member States retain to give priority to the right to privacy or to the right to property is qualified by a number of requirements. Accordingly, when transposing Directives 2000/31, 2001/29, 2002/58 and 2004/48 into national law, it is for the Member States to ensure that they rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Furthermore, when applying the measures transposing those directives, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives, but must also make sure that they do not rely on an interpretation of those directives which would conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality (  
Promusicae  
, paragraph 70).   
29      Accordingly, the answer to the second question is that Community law – in particular, Article 8(3) of Directive 2004/48, read in conjunction with Article 15(1) of Directive 2002/58 – does not preclude Member States from imposing an obligation to disclose to private third parties personal data relating to Internet traffic in order to enable them to bring civil proceedings for copyright infringements. Community law nevertheless requires Member States to ensure that, when transposing Directives 2000/31, 2001/29, 2002/58 and 2004/48 into national law, they rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights involved. Moreover, when applying the measures transposing those directives, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives, but must also make sure that they do not rely on an interpretation of those directives which would conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.  
   
The first question  
30      By its first question, the national court asks, essentially, whether access providers which merely provide users with Internet access, without offering other services or exercising any control, whether   
de iure  
 or   
de facto  
, over the services which users make use of, are ‘intermediaries’ within the meaning of Articles 5(1)(a) and 8(3) of Directive 2001/29.  
31      On the view that the answer to that question admits of no reasonable doubt, the Court informed the national court, in accordance with the second paragraph of Article 104(3) of the Rules of Procedure, that it proposed to give its decision by reasoned order, and called on the interested parties referred to in Article 23 of the Statute of the Court of Justice to submit any observations they might have in that regard.  
32      LSG, the Spanish and United Kingdom Governments and the Commission of the European Communities indicated to the Court that they had no objection to the Court’s proposal to give its decision by reasoned order.  
33      Tele2 confines its observations in that regard, essentially, to those matters already raised in its written pleadings. According to Tele2, Community law accords Internet access providers privileged treatment, in terms of liability, which is incompatible with an unlimited obligation to disclose information. However, those arguments are not such as to lead the Court to rule out the procedural route envisaged.  
34      It follows clearly both from the order for reference and from the wording of the questions referred that, by its first question, the national court wishes to know whether Internet access providers who merely enable the user to access the Internet may be required to provide the information referred to in the second question.  
35      First, it should be pointed out that Article 5(1)(a) of Directive 2001/29 requires Member States to provide for exemptions from reproduction rights.  
36      The point at issue in the dispute before the referring court is whether LSG can rely on a right to information as against Tele2, not whether Tele2 has infringed reproduction rights.  
37      It follows that an interpretation of Article 5(1)(a) of Directive 2001/29 serves no purpose in relation to the outcome of the dispute before the referring court.  
38      Tele2 maintains, inter alia, that intermediaries must be in a position to bring copyright infringements to an end. Internet access providers, on the other hand, in as much as they exercise no control, whether   
de iure  
 or   
de facto  
, over the services accessed by the user, are not capable of bringing such infringements to an end and, accordingly, are not ‘intermediaries’ within the meaning of Directive 2001/29.   
39      It should be noted at the outset that   
Promusicae  
 concerned the communication by Telefónica de España SAU – a commercial undertaking engaged, inter alia, in the provision of Internet access services – of the identities and physical addresses of certain persons to whom it provided such services and whose IP addresses and dates and times of connection were known (  
Promusicae  
, paragraphs 29 and 30).  
40      It is common ground, as is apparent from the question referred and from the facts in   
Promusicae  
, that Telefónica de España SAU was an Internet access provider (  
Promusicae  
, paragraphs 30 and 34).  
41      Accordingly, in holding – in paragraph 70 of   
Promusicae  
 – that Directives 2000/31, 2001/29, 2002/58 and 2004/48 do not require the Member States to impose, in a situation such as that in   
Promusicae  
, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings, the Court did not immediately rule out the possibility that Member States may, pursuant to Article 8(1) of Directive 2004/48, place Internet access providers under a duty of disclosure.  
42      It should also be pointed out that, under Article 8(3) of Directive 2001/29, Member States are to ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.  
43      Access providers who merely enable clients to access the Internet, even without offering other services or exercising any control, whether   
de iure  
 or   
de facto  
, over the services which users make use of, provide a service capable of being used by a third party to infringe a copyright or related right, inasmuch as those access providers supply the user with the connection enabling him to infringe such rights.  
44      Moreover, according to Recital 59 in the preamble to Directive 2001/29, rightholders should have the possibility of applying for an injunction against an intermediary who ‘carries a third party’s infringement of a protected work or other subject-matter in a network’. It is common ground that access providers, in granting access to the Internet, make it possible for such unauthorised material to be transmitted between a subscriber to that service and a third party.  
45      That interpretation is borne out by the aim of Directive 2001/29 which, as is apparent in particular from Article 1(1) thereof, seeks to ensure the legal protection of copyright and related rights in the framework of the internal market. The protection sought by Directive 2001/29 would be substantially diminished if ‘intermediaries’, within the meaning of Article 8(3) of that directive, were to be construed as not covering access providers, which alone are in possession of the data making it possible to identify the users who have infringed those rights.  
46      In view of the foregoing, the answer to the first question is that access providers which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether   
de iure  
 or   
de facto  
, over the services which users make use of, must be regarded as ‘intermediaries’ within the meaning of Article 8(3) of Directive 2001/29.  
   
Costs  
47      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.   
On those grounds, the Court (Eighth Chamber) hereby rules:  
1.        
Community law – in particular, Article 8(3) of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, read in conjunction with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) – does not preclude Member States from imposing an obligation to disclose to private third parties personal data relating to Internet traffic in order to enable them to bring civil proceedings for copyright infringements. Community law nevertheless requires Member States to ensure that, when transposing into national law Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, and Directives 2002/58 and 2004/48, they rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights involved. Moreover, when applying the measures transposing those directives, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives but must also make sure that they do not rely on an interpretation of those directives which would conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.  
2.        
Access providers which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether   
de iure  
 or   
de facto  
, over the services which users make use of, must be regarded as ‘intermediaries’ within the meaning of Article 8(3) of Directive 2001/29.

ID: 95564f48-37ef-4212-b55a-ae60f818182e

of 8 Dec 2022, C-180/21 (  
Inspektor v Inspektorata kam Visshia sadeben savet  
)  
Law Enforcement Directive   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
Law Enforcement Directive   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
   
JUDGMENT OF THE COURT (Fifth Chamber)  
8 December 2022 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Articles 2, 4 and 6 – Applicability of Regulation 2016/679 – Concept of ‘legitimate interest’ – Concept of ‘task carried out in the public interest or in the exercise of official authority’ – Directive (EU) 2016/680 – Articles 1, 3, 4, 6 and 9 – Lawfulness of the processing of personal data collected in the course of a criminal investigation – Subsequent processing of data relating to a presumed victim of a criminal offence for the purpose of making a formal accusation in respect of him or her – Concept of purpose ‘other than that for which the personal data are collected’ – Data used by the public prosecutor’s office of a Member State for the purposes of its defence in an action for damages against the State)  
In Case C-180/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Administrativen sad – Blagoevgrad (Administrative Court, Blagoevgrad, Bulgaria), made by decision of 19 March 2021, received at the Court on 23 March 2021, in the proceedings  
VS  
v  
Inspektor v Inspektorata kam Visshia sadeben savet,  
interested party:  
Teritorialno otdelenie – Petrich kam Rayonna prokuratura – Blagoevgrad,  
THE COURT (Fifth Chamber),  
composed of E. Regan, President of the Chamber, D. Gratsias (Rapporteur), M. Ilešič, I. Jarukaitis, and Z. Csehi, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        VS, by V. Harizanova,  
–        Inspektor v Inspektorata kam Visshia sadeben savet, by S. Mulyachka,   
–        the Bulgarian Government, by M. Georgieva and T. Mitova, acting as Agents,  
–        the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
–        the Netherlands Government, by M.K. Bulterman and J.M. Hoogveld, acting as Agents,  
–        the European Commission, by H. Kranenborg and I. Zaloguin, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 19 May 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 1(1) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89) and of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2006 L 119, p. 1; ‘the GDPR’), in particular Article 6(1) thereof.  
2        The request has been made in proceedings between VS and Inspektor v Inspektorata kam Visshia sadeben savet (Inspector with the Inspectorate at the Supreme Judicial Council, Bulgaria) (‘the IVSS’) concerning the lawfulness of the processing of personal data concerning VS by the District Public Prosecutor’s Office, Petrich (Bulgaria).  
   
Legal context  
   
European Union law  
   
The GDPR  
3        Recitals 19, 45 and 47 of the GDPR state:  
‘(19)      … Member States may entrust competent authorities within the meaning of [Directive 2016/680] with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.  
…  
…  
(45)      Where processing is … necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. …  
…  
(47)      The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. … Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. …’  
4        Article 2 of that regulation, entitled ‘Material scope’, provides, in paragraphs 1 and 2:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
…  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
5        Article 4 of the GDPR, entitled ‘Definitions’, provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;  
…’  
6        Article 5 of the GDPR, entitled ‘Principles relating to processing of personal data’, provides, in paragraph 1:  
‘Personal data shall be:  
…  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; … (“purpose limitation”);  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
…’  
7        Under Article 6 of the GDPR, entitled ‘Lawfulness of processing’:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data …  
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.  
…  
3.      The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.  
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. …’  
8        Article 21 of the GDPR, entitled ‘Right to object’, provides, in paragraph 1:  
‘The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) … The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.’  
9        Article 23 of that regulation, entitled ‘Restrictions’, states, in paragraph 1, that EU or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, inter alia, certain important objectives of general public interest of the European Union or of a Member State.  
   
Directive 2016/680  
10      Recitals 8 to 12, 27 and 29 of Directive 2016/680 state:  
‘(8)      Article 16(2) TFEU mandates the European Parliament and the Council [of the European Union] to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.  
(9)      On that basis, [the GDPR] lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union.  
(10)      In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.  
(11)      It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, [the GDPR] therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. …  
(12)      The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. … Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of [the GDPR].  
…  
(27) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.  
…  
(29)      Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. If personal data are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose.’  
11      Article 1 of that directive, entitled ‘Subject matter and objectives’, provides, in paragraph 1:  
‘This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
12      The definitions of the terms ‘personal data’ and ‘processing’ in paragraphs 1 and 2, respectively, of Article 3 of that directive, entitled ‘Definitions’, reproduce those set out in Article 4(1) and (2) of the GDPR.  
13      Under Article 3(7)(a) and (8) of Directive 2016/680:  
‘For the purposes of this Directive:  
…  
(7)      “competent authority” means:  
(a)      any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; …  
…  
(8)      “controller” means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law’.  
14      Article 4 of Directive 2016/680, entitled ‘Principles relating to processing of personal data’, states, in paragraph 1:  
‘Member States shall provide for personal data to be:  
…  
(b)      collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are processed;  
…’  
15      Article 4(2) of Directive 2016/680 provides:  
‘Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:  
(a)      the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and  
(b)      processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.’  
16      Under Article 6 of Directive 2016/680, entitled ‘Distinction between different categories of data subject’:  
‘Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:  
(a)      persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;  
(b)      persons convicted of a criminal offence;  
(c)      victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; …  
…’  
17      Article 9 of Directive 2016/680, entitled ‘Specific processing conditions’, provides, in paragraphs 1 and 2:  
‘1.      Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, [the GDPR] shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.  
2.      Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), [the GDPR] shall apply to processing for such purposes …, unless the processing is carried out in an activity which falls outside the scope of Union law.’  
   
Bulgarian law  
   
Constitution of the Republic of Bulgaria  
18      Article 127 of the Constitution of the Republic of Bulgaria provides:  
‘The Public Prosecutor’s Office shall ensure that laws are complied with by:  
1.      directing the investigation and reviewing the lawfulness of its conduct;  
2.      having the powers to conduct an investigation;  
3.      making a formal accusation in respect of persons who have committed criminal offences and prosecuting criminal offences subject to public prosecution;  
…’  
   
The ZZLD  
19      In accordance with Article 1 thereof, the Zakon za zashtita na lichnite danni (Law on the Protection of Personal Data) (DV No 1 of 4 January 2002; ‘the ZZLD’) seeks to ensure the protection of natural persons with regard to the processing of personal data as governed by the GDPR and with regard to the processing of such data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public order and security.  
20      In accordance with Article 17(1) of the ZZLD, the IVSS is to monitor and ensure compliance with the GDPR, the ZZLD and acts on the subject of the protection of personal data in the processing of personal data by, inter alia, the Public Prosecutor’s Office and the investigating authorities in the exercise of their judicial functions, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Article 38b of the ZZLD confers on the data subject, in the event of an infringement of his or her rights, inter alia by those authorities, the right to lodge a complaint with the IVSS.  
21      Article 42(2) and (3), Article 45(2) and Article 47 of the ZZLD implement Article 9(1) and (2), Article 4(2) and Article 6 of Directive 2016/680 respectively.  
   
The Code of Criminal Procedure  
22      Article 191 of the Nakazatelno-protsesualen kodeks (Code of Criminal Procedure) (DV No 86 of 28 October 2005), in the version applicable to the dispute in the main proceedings, provides:  
‘Pre-trial proceedings shall be conducted in respect of criminal offences subject to public prosecution.’  
23      Article 192 of the Code of Criminal Procedure, in the version applicable to the dispute in the main proceedings, provides:  
‘Pre-trial proceedings shall comprise an investigation and actions of the Public Prosecutor after the investigation has been closed.’  
   
The Code of Civil Procedure  
24      Articles 8 and 9 of the Grazhdanski protsesualen kodeks (Code of Civil Procedure) (DV No 59 of 20 July 2007), in the version applicable to the dispute in the main proceedings, implement the principles of   
audi alteram partem  
 and equality of arms respectively.  
25      Article 154 of the Code of Civil Procedure, in the version applicable to the dispute in the main proceedings, entitled ‘Burden of proof’, provides, in paragraph 1:  
‘Each party shall be required to establish the facts on which it bases its claims or objections.’  
   
The Zakon za otgovornostta na darzhavata i obshtinite za vredi   
26      Article 2b of the Zakon za otgovornostta na darzhavata i obshtinite za vredi (Law on liability of the State and of municipalities for damage) (DV No 60 of 5 August 1988) provides:  
‘(1) The State shall be liable for damage caused to citizens and legal persons by an infringement of the right to have the case examined and disposed of within a reasonable time in accordance with Article 6(1) of the Convention [for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950].  
(2) The actions referred to in paragraph 1 shall be examined in accordance with the Code of Civil Procedure, whereby the court shall take into account the total duration and subject matter of the proceedings, their factual and legal complexity, the conduct of the parties and of their procedural or legal representatives, the conduct of the other parties to the proceedings and of the competent authorities, and other facts relevant to the correct resolution of the dispute.  
…’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
27      In 2013, the District Public Prosecutor’s Office, Petrich, opened pre-trial proceedings No 252/2013 against an unknown person for the commission of an offence referred to in Article 325(1) of the Nakazatelen kodeks (Criminal Code), read in conjunction with Article 20(2) thereof, in the context of an incident which took place in a bar. The applicant in the main proceedings, VS, took part in those proceedings as a victim of that criminal offence.  
28      In 2016, following a number of complaints concerning, inter alia, VS, the District Public Prosecutor’s Office, Petrich, compiled a number of files containing information relating to that person, but did not open any pre-trial proceedings in the absence of evidence that a criminal offence had been committed.  
29      In 2018, in the context of pre-trial proceedings No 252/2013, the public prosecutor made formal accusations in respect of all the persons who took part in the incident at issue in those proceedings, including VS.   
30      In civil proceedings, VS brought an action before the Okrazhen sad Blagoevgrad (Regional Court, Blagoevgrad, Bulgaria) against the Public Prosecutor’s Office of the Republic of Bulgaria seeking damages for the harm allegedly resulting from the excessive duration of pre-trial proceedings No 252/2013. At the hearing on 15 October 2018, for the purposes of defending that public prosecutor’s office, a public prosecutor of the District Public Prosecutor’s Office, Petrich, representing the Public Prosecutor’s Office, requested that the files opened by that public prosecutor’s office in 2016, referred to in paragraph 28 of this judgment, be produced in the context of that action. It is apparent from the order for reference that that public prosecutor thus intended to demonstrate that the health problems relied on by the applicant in the main proceedings were not, as he claimed, attributable to those pre-trial proceedings, but had been caused by the checks carried out by the police and by the District Public Prosecutor’s Office, Petrich, in connection with those files. At the same hearing, the Okrazhen sad Blagoevgrad (Regional Court, Blagoevgrad) ordered that public prosecutor’s office to produce certified copies of the documents in the files in question, which the public prosecutor of that public prosecutor’s office then did.  
31      On 12 March 2020, VS lodged a complaint with the IVSS, claiming that the District Public Prosecutor’s Office, Petrich, had infringed the provisions relating to the protection of personal data. By his first claim, he submitted that that public prosecutor’s office had unlawfully used his personal data, which had been collected when he was considered to be a victim of a criminal offence, in order to prosecute him in the same proceedings and in respect of the same acts. By his second claim, he alleged that the public prosecutor’s office acted unlawfully as regards the processing of personal data that were collected in the files referred to in paragraph 28 of this judgment, in the context of his action for damages against the Public Prosecutor’s Office of the Republic of Bulgaria. By decision of 22 June 2020, the IVSS rejected that complaint.  
32      On 31 July 2020, VS brought an action before the referring court against that decision, claiming, first, that the processing of his personal data in the course of pre-trial proceedings No 252/2013 is contrary to, inter alia, the principles of Directive 2016/680, and second, that the processing of the data collected in the files referred to in paragraph 28 of this judgment, after the Public Prosecutor’s Office had refused to initiate pre-trial proceedings, infringes the principles of the GDPR.  
33      Taking the view, in the light of the Court’s case-law, that the dispute in the main proceedings concerns the processing of personal data in the context of activities coming within the scope of the GDPR and Directive 2016/680, the referring court has doubts as to the limits laid down by EU law concerning the subsequent processing of personal data that were initially collected by the controller for the purposes of the investigation and detection of a criminal offence.  
34      In particular, first, the referring court has doubts whether, in the event that the Public Prosecutor’s Office of the Republic of Bulgaria, as a ‘competent authority’ within the meaning of Article 3(7)(a) of Directive 2016/680, and as a ‘controller’ within the meaning of Article 3(8) of that directive, has collected, for the purposes of the investigation and detection of a criminal offence, personal data relating to a person who was considered to be a victim at the time of that collection, the subsequent processing of those data by the same authority for the purposes of the prosecution of that person serves a purpose that comes within the scope of that directive but that is other than that for which the data in question was collected, within the meaning of Article 4(2) of that directive.  
35      Second, the referring court states that the reference, in the context of the action for damages brought by VS, to the information relating to that person contained in the files opened in 2016 by the District Public Prosecutor’s Office, Petrich, serves a different purpose from that for which that information was collected and states that, in the context of that action, the Public Prosecutor’s Office, as defendant, is not acting for the purposes of the prevention, investigation, detection or prosecution of criminal offences. However, the referring court has doubts whether the mere fact of indicating to the civil court having jurisdiction that those files concern VS and of transmitting to it that information in full or in part constitutes ‘processing’ of ‘personal data’, within the meaning of Article 4(1) and (2) of the GDPR, coming within the scope of that regulation, in accordance with Article 2(1) thereof.  
36      Furthermore, the referring court considers, in essence, that the dispute in the main proceedings raises the question of reconciling the protection of personal data and the rights of a party to judicial proceedings, where those data have been collected by that party in its capacity as controller within the meaning of Article 3(8) of Directive 2016/680, in particular in the light of point (f) of the first subparagraph of Article 6(1) of the GDPR relating to the necessity of processing for the purposes of the legitimate interests pursued by that controller.   
37      The referring court considers that the other grounds for lawfulness of the processing of personal data coming within the scope of the GDPR, which are set out in the first subparagraph of Article 6(1) of that regulation, are not relevant in the dispute in the main proceedings. In particular, according to that court, the provision, for the purposes of its defence in civil proceedings, by the Public Prosecutor’s Office to the court having jurisdiction of information relating to the criminal files opened by it is not necessary for the performance of a task carried out in the public interest and is not covered by the exercise of official authority within the meaning of point (e) of the first subparagraph of Article 6(1) of that regulation.  
38      In those circumstances, the Administrativen sad – Blagoevgrad (Administrative Court, Blagoevgrad) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 1(1) of [Directive 2016/680] to be interpreted as meaning that, when stating the objectives of that directive, the terms “prevention, investigation, detection or prosecution of criminal offences [or the execution of criminal penalties]” are listed as aspects of a general objective?  
(2)(a)      Are the provisions of [the GDPR] applicable to the Public Prosecutor’s Office of the Republic of Bulgaria in view of the fact that information concerning a person, which was collected by the Public Prosecutor’s Office, in its capacity as “controller” pursuant to point 8 of Article 3 of [Directive 2016/680], in an investigation file opened in relation to that person with a view to verifying indications of a criminal offence, was used in the context of the judicial defence of the Public Prosecutor’s Office as a party to civil proceedings – by virtue of the fact that the circumstance of that file having been opened was revealed or that the contents of the file were presented?  
(b)      If that question is answered in the affirmative: Is the expression “legitimate interests” in [point (f) of the first subparagraph of Article 6(1) of the GDPR] to be interpreted as including the disclosure, in whole or in part, of information concerning a person which has been collected in a public prosecution investigation file opened in relation to that person for the purposes of the prevention, investigation, detection or prosecution of criminal offences, in the case where that disclosure is carried out for the purposes of the defence of the controller as a party to civil proceedings, and does that expression exclude the consent of the data subject?’  
   
Consideration of the questions referred  
   
The first question  
39      As a preliminary point, it should be noted that, even if the referring court formally confined its first question to the interpretation of Article 1(1) of Directive 2016/680, that circumstance does not prevent the Court from providing it with all the elements of interpretation which may be useful for the judgment in the main proceedings, by extracting from the body of material provided by that court, and in particular from the statement of reasons for the order for reference, the elements of EU law which require interpretation in the light of the subject matter of the dispute (see, to that effect, judgment of 22 April 2021,   
Profi Credit Slovakia  
, C-485/19, EU:C:2021:313, paragraph 50 and the case-law cited).  
40      It follows that, by its first question, the referring court seeks, in essence, to ascertain (i) whether Article 1(1) of Directive 2016/680, read in conjunction with Article 4(2) and Article 6 thereof, must be interpreted as meaning that the processing of personal data serves a purpose other than that for which those data were collected, where such data were collected for the purposes of the detection and investigation of a criminal offence and the data subject was, at the time of that collection, considered to be a victim, but that processing is carried out for the purpose of prosecuting that person following the conclusion of the criminal investigation at issue, and, (ii) as the case may be, whether that processing is permitted.  
41      According to settled case-law, it is necessary, for the interpretation of a provision of EU law, that account be taken not only of its wording, but also of its context and the objectives pursued by the rules of which it is part. The origins of a provision of EU law may also provide information relevant to its interpretation (see, to that effect, judgment of 1 October 2019,   
Planet49  
, C-673/17, EU:C:2019:801, paragraph 48 and the case-law cited).  
42      In the first place, it must be noted, first of all, that the wording of Article 1(1) of Directive 2016/680, which relates to the subject matter of that directive, expressly distinguishes between different categories of activities whose purposes the processing of the relevant personal data may serve. In that regard, it is apparent from the various language versions of that provision, in particular those in Bulgarian, Spanish, German, Greek, English and Italian, that the different purposes referred to in Article 1(1) of that directive correspond to the ‘prevention’, ‘detection’, ‘investigation’ and ‘prosecution’ of criminal offences and ‘the execution of criminal penalties’, including the ‘safeguarding’ against ‘threats to public security’ and the ‘prevention’ of such threats.  
43      Next, the wording of Article 4(2) of that directive, which states that processing for ‘any of the purposes set out in Article 1(1) [thereof] other than that for which the personal data are collected’ is to be permitted, subject to compliance with the requirements laid down by that provision, expressly confirms that the terms listed in Article 1(1), namely ‘prevention’, ‘investigation’, ‘detection’ ‘prosecution’, ‘execution of criminal penalties’, ‘safeguarding against [threats to public security]’ and ‘the prevention of threats to public security’ concern several separate purposes of the processing of personal data coming within the scope of that directive.  
44      It can thus be inferred from the very wording of Article 1(1) of Directive 2016/680, read in conjunction with Article 4(2) thereof, that, where personal data have been collected for the purposes of the ‘detection’ and ‘investigation’ of a criminal offence and have subsequently been processed for the purposes of ‘prosecution’, that collection and that processing serve different purposes.  
45      Lastly, it must be observed that, under Article 6 of that directive, Member States are under an obligation to provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as, inter alia, those referred to in points (a), (b) and (c) of that article, namely, respectively, persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence, persons convicted of a criminal offence, and victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence.  
46      Consequently, a person whose personal data are processed for the purposes of criminal prosecution must be regarded as coming within the category of persons with regard to whom there are serious grounds for believing that they have committed a criminal offence, within the meaning of Article 6(a) of Directive 2016/680. It follows that, if, as in the situation referred to in the first question, that person had initially been considered to be a victim of a criminal offence, within the meaning of Article 6(c) of that directive, that processing therefore reflects a change in that person’s category, which it is for the controller to take into account in accordance with the requirement laid down in that article to make a clear distinction between data of different categories of persons.  
47      That said, it must be stated that neither Article 1(1) of Directive 2016/680 nor Article 4(2) thereof refers to Article 6 of that directive or to its content in order to lay down the purpose of the processing of personal data coming within the scope of that directive.  
48      Moreover, as the Advocate General observed, in essence, in point 62 of his Opinion, the expression ‘where applicable and as far as possible’, used in Article 6 of Directive 2016/680, clearly indicates that it is not necessarily possible to draw a clear distinction between such data, in particular where, as in the present case, those data are collected for the purposes of an ‘investigation’ or ‘detection’ of a criminal offence, since the same person may come within several categories of persons as referred to in Article 6 of that directive and the determination of the categories concerned might change in the course of the pre-trial proceedings, in accordance with the gradual clarification of the facts at issue.  
49      It must be inferred from this that Article 6 lays down an obligation that is separate from that laid down in Article 4(2) and, as the Advocate General noted in points 61 to 64 of his Opinion, that obligation is not relevant for the purpose of determining whether the processing of personal data serves a purpose other than that for which those data were collected, within the meaning of that provision.  
50      In the second place, as regards the context of the legislation at issue, it should be noted that Article 4(1)(b) and (c) of Directive 2016/680 provides, first, that personal data must be collected for specified, explicit and legitimate purposes and not be processed in a manner that is incompatible with those purposes, and second, that those data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. Those two requirements are set out, in essence, in the same terms in Article 5(1)(b) and (c) of the GDPR, which states that they correspond to the principles of purpose limitation and data minimisation, respectively.  
51      That said, it must be observed that Article 4(2) of that directive, in the light of recital 29 thereof, authorises subsequent processing of personal data for a purpose other than that for which those data were collected, where that purpose is among those set out in Article 1(1) of that directive and that processing satisfies the two conditions laid down in Article 4(2)(a) and (b). First, the controller must be authorised to process such personal data for such a purpose in accordance with EU or Member State law. Second, processing must be necessary and proportionate to that other purpose.  
52      In particular, personal data collected for the purposes of the ‘prevention’ and ‘detection’ or ‘investigation’ of criminal offences may be processed subsequently, where appropriate, by different competent authorities, for the purposes of ‘prosecution’ or the ‘execution of criminal penalties’, where a criminal offence has been identified and consequently calls for law enforcement action.  
53      However, in the context of the collection of personal data for the purposes of the ‘detection’ and ‘investigation’ of criminal offences, the competent authorities are required to gather any data that are potentially relevant to the determination of the acts constituting the criminal offence at issue at a stage where those acts have not yet been established. By contrast, in the context of the processing of personal data for the purposes of ‘prosecution’, those data aim to establish that the acts attributed to the accused persons have sufficient probative value and that the classification of those acts under criminal law is accurate, in order to enable the court having jurisdiction to give a ruling.  
54      Consequently, first, personal data necessary for the purposes of the ‘detection’ and ‘investigation’ of a criminal offence will not be systematically necessary for the purposes of ‘prosecution’. Second, the consequences of the processing of personal data for the data subjects might be substantially different, as regards, in particular, the degree of interference with their right to the protection of those data and the effects of that processing on their legal situation in the criminal proceedings in question.  
55      In addition, it should be noted that the scope of Article 4(2) is not limited to the processing of personal data in connection with the same criminal offence as that warranting the collection of those data. As stated in recital 27 of Directive 2016/680, that directive takes account of the need for the authorities responsible for combating criminal offences to process personal data for a purpose other than that which led to the collection of those data, in particular with the aim of developing an understanding of criminal activities and of making links between different criminal offences detected.  
56      It follows from the foregoing that, in order to meet the requirements referred to in Article 4(2)(a) and (b) of Directive 2016/680, the assessment of compliance with those requirements in the processing, by the same or by another controller, of personal data for one of the purposes set out in Article 1(1), other than that for which those data were collected, must be carried out by regarding each of the purposes referred to in Article 1(1) as specific and distinct.  
57      In the third place, as regards the objectives of the legislation at issue, it should be noted that, as is apparent from recitals 10 and 11 of Directive 2016/680, the EU legislature sought to adopt rules which take account of the specific nature of the field covered by that directive.   
58      In that regard, recital 12 states that the activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not.  
59      It follows from this that the EU legislature sought to adopt rules corresponding to the specific features which characterise the activities carried out by the competent authorities in the field governed by that directive, while taking account of the fact that they constitute distinct activities serving purposes specific to them.  
60      This interpretation, in the light of the context of the provision at issue and the objectives pursued by the legislation of which it is part, is borne out by its origins, in particular by the statement of the Council’s reasons concerning Council Position (EU) No 5/2016 at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 C 158, p. 46). In that statement of reasons, the Council explains the insertion of that provision into Directive 2016/680 by stating that it ‘enables, for example, [a] prosecutor to process the same personal data for the prosecution of a crime, as the police did for the detection of a crime given that both purposes in the example are covered by Article 1(1) [of that directive]’.  
61      It is therefore for the referring court to determine, with a view to resolving the dispute in the main proceedings, whether the processing of personal data concerning VS by the District Public Prosecutor’s Office, Petrich, for the purpose of prosecuting that person, could be permitted in the light of the conditions laid down in Article 4(2) of Directive 2016/680, by ascertaining, first, whether that authority was authorised under Bulgarian criminal law to carry out that processing and, second, whether that processing was necessary and proportionate to its purpose.  
62      In that regard, it should be noted that, for the purpose of assessing whether that processing is necessary and proportionate, the referring court may, where appropriate, take account of the fact that the authority responsible for that prosecution must be in a position to rely on the data collected during that investigation as evidence of the acts constituting the offence, in particular those relating to the persons involved therein, provided that those data are necessary to identify those persons and to establish their involvement.  
63      In the light of all the foregoing, the answer to the first question is that Article 1(1) of Directive 2016/680, read in conjunction with Article 4(2) and Article 6 thereof, must be interpreted as meaning (i) that the processing of personal data serves a purpose other than that for which those data were collected, where such data were collected for the purposes of the detection and investigation of a criminal offence, but that processing is carried out for the purpose of prosecuting a person following the conclusion of the criminal investigation at issue, irrespective of the fact that that person was considered to be a victim at the time of that collection, and (ii) that such processing is permitted pursuant to Article 4(2) of that directive, provided that it meets the conditions laid down in that provision.  
   
The second question  
64      By its second question, the referring court asks, in essence, first, whether Article 3(8) and Article 9(1) and (2) of Directive 2016/680 and Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation is applicable to the processing of personal data by the public prosecutor’s office of a Member State for the purpose of exercising its rights of defence in an action for damages against the State, where it informs the court having jurisdiction of the existence of files concerning a natural person who is a party to that action, opened for the purposes set out in Article 1(1) of that directive, and transmits those files to that court and, second, if that question were to be answered in the affirmative, whether point (f) of the first subparagraph of Article 6(1) of that regulation must be interpreted as meaning that such processing of personal data may be regarded as lawful for the purposes of the legitimate interests pursued by the controller, within the meaning of that provision.  
   
Admissibility  
65      In its written observations, the IVSS disputes the admissibility of the second question on the ground that it was raised by the referring court in the context of the examination of a claim put forward by VS which had been rejected as inadmissible by the decision that is the subject matter of the dispute in the main proceedings, on account of the expiry of the statutory time limit for raising it.  
66      According to the Court’s settled case-law, questions on the interpretation of EU law referred by a national court in the factual and legislative context which that court is responsible for defining, and the accuracy of which is not a matter for the Court to determine, enjoy a presumption of relevance. The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought is unrelated to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see, to that effect, judgment of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraph 50 and the case-law cited).  
67      In the present case, it should be noted, as the Advocate General observed in points 76 and 77 of his Opinion, that the matter of the admissibility of the claims raised by VS in his complaint before the IVSS comes entirely within the jurisdiction of the referring court. Moreover, in the order for reference, that court stated that it considered the second question to be relevant, notwithstanding IVSS’ rejection of the claim referred to in paragraph 65 of this judgment as inadmissible. It is not, in any event, for the Court of Justice to re-examine that assessment.  
68      It follows that the second question is admissible.  
   
Substance  
–         
The application of the GDPR to the processing of personal data by the public prosecutor’s office of a Member State for the purpose of exercising its rights of defence in an action for damages against the State  
69      In the first place, it is necessary to determine whether the use, by the public prosecutor’s office of a Member State, of information concerning a natural person that it has collected and processed for purposes coming within the scope of Article 1(1) of Directive 2016/680, with a view to exercising its rights of defence in civil proceedings, constitutes ‘processing’ of ‘personal data’ within the meaning of Article 4(1) and (2) of the GDPR.  
70      First of all, it must be borne in mind that ‘personal data’, within the meaning of Article 4(1) of the GDPR, means ‘any information relating to an identified or identifiable natural person’, it being understood that, according to the case-law, that definition is applicable where, by reason of its content, purpose and effect, the information in question is linked to a particular person (see, to that effect, judgment of 20 December 2017,   
Nowak  
, C-434/16, EU:C:2017:994, paragraph 35). Furthermore, under Article 4(2) of the GDPR, the concept of ‘processing’ is defined as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means’ such as, inter alia, ‘consultation’, ‘use’, ‘disclosure by transmission’, ‘dissemination’ or ‘otherwise making available’. Those definitions reflect the aim of the EU legislature to assign a broad scope to those two concepts (see, to that effect, judgments of 20 December 2017,   
Nowak  
, C-434/16, EU:C:2017:994, paragraph 34, and of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 35).  
71      In that regard, first, the fact that the defendant in civil proceedings informs the court having jurisdiction, even succinctly, in its written pleadings or at the hearing, of the opening of files concerning the natural person who has brought those proceedings, in particular for the purposes of the ‘detection’ or ‘investigation’ of a criminal offence, means that that defendant ‘consulted’, ‘used’ and ‘transmitted’ or ‘disclosed’ ‘personal data’ for the purposes of Article 4(1) and (2) of the GDPR. Thus, both in terms of its content and its purpose and effect, that information is linked to a particular person, who is identifiable both by the party that disclosed it and by the court to which it is transmitted.  
72      Second, the fact that that defendant produces, at the request of the court having jurisdiction, files relating to procedures concerning that natural person involves, at the very least, the ‘use’ and ‘disclosure by transmission’ of ‘personal data’ within the meaning of Article 4(1) and (2) of the GDPR.  
73      In the second place, it must be borne in mind that Article 2(1) of the GDPR defines broadly the material scope of that regulation (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 61), which includes any ‘processing of personal data wholly or partly by automated means and … the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system’. The corollary of that broad definition is that the exceptions to the application of the GDPR listed in Article 2(2) thereof must be interpreted strictly. That is the case, in particular, with the exception provided for in Article 2(2)(d) which concerns the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (see, to that effect, judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraphs 40 and 41 and the case-law cited).  
74      In that regard, the Court has held that, as follows from recital 19 of that regulation, the reason for that exception is that the processing of personal data by the competent authorities for the purposes set out in Article 2(2)(d) of the GDPR is governed by a specific EU legal act, namely Directive 2016/680, which was adopted on the same day as the GDPR (see, to that effect, judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 42 and the case-law cited).  
75      As is apparent from recital 12 of Directive 2016/680, the EU legislature laid down, in Article 9 of that directive, rules relating to the processing of personal data for purposes other than those set out in Article 1(1) of that directive, for which those data were collected.  
76      In that regard, Article 9(1) of Directive 2016/680 provides, first, that such processing of personal data cannot, in principle, be carried out, unless it is authorised by EU or Member State law and, second, that the GDPR is to apply to that processing, unless the processing is carried out in an activity which falls outside the scope of EU law. Furthermore, under Article 9(2) of that directive, unless the processing is carried out in such an activity, the GDPR is to apply to the processing by the competent authorities in the performance of their tasks other than those performed for the purposes set out in Article 1(1) of that directive.  
77      In the situations referred to in paragraphs 71 and 72 of this judgment, the collection and processing of personal data by the public prosecutor’s office of a Member State for the purposes of the ‘prevention’, ‘detection’, ‘investigation’ or ‘prosecution’ of a criminal offence certainly constitute processing of personal data for the purposes set out in Article 1(1) of Directive 2016/680, within the meaning of Article 9(1) and (2) of that directive.  
78      However, even where the bringing of an action for damages against the State arises from alleged misconduct on the part of the public prosecutor’s office in the course of criminal proceedings, such as, as in the present case, alleged infringements of the right to be tried within a reasonable time, the aim of the State’s defence in such an action is not to perform, as such, that public prosecutor office’s tasks for the purposes set out in Article 1(1) of Directive 2016/680.  
79      Furthermore, in the light of the principle that exceptions to the application of the GDPR must be interpreted strictly, that processing of personal data cannot be regarded as being carried out ‘in an activity which falls outside the scope of Union law’, within the meaning of Article 2(2)(a) of the GDPR and Article 9(1) and (2) of Directive 2016/680. In that regard, it follows from the case-law that the sole purpose of that expression is to exclude from the scope of the GDPR the processing of personal data carried out by the State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category. The participation of a public authority in civil proceedings as a defendant in an action for damages against the State does not seek to safeguard national security; nor can it be classified in the same category of activities (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraphs 66 to 68 and the case-law cited).  
80      In the third place, it should be noted that, for the purpose of applying the GDPR to the data processing referred to in paragraphs 71 and 72 of this judgment, the public prosecutor’s office must be considered to be a ‘controller’, within the meaning not only of Article 4(7) of the GDPR, but also of Article 3(8) of Directive 2016/680, in that ‘alone or jointly with others’, it ‘determines the purposes and means’ of that processing, within the meaning of the latter provision. It is that authority, as a party to the proceedings, which informs the court having jurisdiction of the existence of files opened in criminal matters concerning the other party and which transmits those files to it. Its status as ‘controller’, having regard to the broad definition of that concept, which seeks to ensure effective and complete protection of data subjects, is independent of the extent of its involvement and its level of responsibility, which may be different from those of the court having jurisdiction, for which it is to authorise or order such processing (see, by analogy, judgment of 29 July 2019,   
Fashion ID  
, C-40/17, EU:C:2019:629, paragraphs 66 to 70).  
81      Irrespective of whether the data processing referred to in paragraph 80 of this judgment comes within the scope of Article 9(1) or (2) of Directive 2016/680, it is apparent from the wording of those paragraphs and the relationship between them that the GDPR applies to any processing of personal data, collected for the purposes set out in Article 1(1) of that directive, for other purposes, unless the processing in question falls outside the scope of EU law, including where the ‘controller’, within the meaning of Article 3(8) of that directive, is a ‘competent authority’ within the meaning of Article 3(7)(a) thereof and carries out the processing of personal data in the context of tasks other than those performed for the purposes set out in Article 1(1) of that directive.  
82      In the light of all the foregoing, it must be held that the GDPR is applicable to the processing of personal data by the public prosecutor’s office of a Member State for the purpose of exercising its rights of defence in an action for damages against the State, where, first, it informs the court having jurisdiction of the opening of files relating to a natural person who is a party to that action for the purposes set out in Article 1(1) of Directive 2016/680 and, second, it transmits those files to that court.  
–         
The lawfulness of the processing of personal data by the public prosecutor’s office of a Member State for the purpose of exercising its rights of defence in an action for damages against the State  
83      It must be borne in mind that Article 6 of the GDPR lists, in a restrictive manner, the cases in which processing of personal data can be regarded as lawful (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 99).  
84      Those cases include point (e) of the first subparagraph of Article 6(1) of the GDPR, which makes provision for processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and point (f) of the first subparagraph of Article 6(1) of that regulation, which refers to processing that is necessary for the purposes of the legitimate interests or freedoms pursued by the controller or by a third party, unless the interests or fundamental rights and freedoms of the data subject require the protection of personal data. According to the second subparagraph of Article 6(1) of that regulation, point (f) of the first subparagraph of Article 6(1) thereof is not to apply to processing carried out by public authorities in the performance of their tasks.  
85      It should be noted that, as the Commission correctly stated in its written observations, it is clear from the wording of the second subparagraph of Article 6(1) of the GDPR that the processing of personal data by a public authority in the performance of its tasks cannot come within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR, relating to the processing of personal data that is necessary for the purposes of the legitimate interests pursued by the controller. As follows from recital 47 of the GDPR and as the Commission has claimed, that latter provision cannot apply to such data processing, since the legal basis of that processing must be provided for by the legislature. It follows that, where processing by a public authority is necessary for the performance of a task in the public interest, and therefore comes within scope of the tasks referred to in the second subparagraph of Article 6(1) of that regulation, the application of point (e) of the first subparagraph of Article 6(1) of the GDPR and that of point (f) of the first subparagraph of Article 6(1) of the GDPR are mutually exclusive.  
86      It is therefore necessary, before considering the matter of the application of point (f) of the first subparagraph of Article 6(1) of the GDPR, to determine whether the processing, by the public prosecutor’s office of a Member State, of personal data initially collected for one or more of the purposes set out in Article 1(1) of Directive 2016/680, for the purpose of defending the State or a public body in an action for damages for harm caused by misconduct on the part of the State or a public body, is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in it, within the meaning of point (e) of the first subparagraph of Article 6(1).   
87      As the Advocate General observed, in essence, in points 94 and 100 of his Opinion, where it is for the public prosecutor’s office to defend the legal and financial interests of the State in an action for damages which calls into question the acts or conduct of that public authority in its performance of tasks in the public interest with which it is entrusted in criminal matters, the defence of those interests may constitute, pursuant to national law, a task carried out in the public interest within the meaning of point (e) of the first subparagraph of Article 6(1) of that regulation.  
88      First, by exercising the procedural rights that it enjoys as defendant, that public authority preserves the legal certainty of the acts carried out and decisions adopted in the public interest that are being called into question by the applicant. The public authority’s submissions concerning the applicant’s claims and arguments are capable of preventing, as the case may be, the risk that those claims and arguments might undermine the effective application of rules on the part of the public authority in the performance of the tasks concerning which improper performance is alleged.  
89      Second, by its claims and arguments in defence, that public authority is capable of pointing, where such is the case, to the potentially unfounded or excessive nature of the applicant’s claims for compensation, with a view, in particular, to preventing the performance of the tasks carried out in the public interest that are being called into question in the action for damages from being hindered by the prospect of actions for damages, where those tasks are liable to harm the interests of individuals.  
90      In that regard, it is irrelevant that, in an action for damages against the State, the public prosecutor’s office is, in its capacity as defendant, on an equal footing with the other parties, and does not exercise public powers, as is the case in the performance of its tasks in criminal matters.  
91      In the present case, it is apparent from the order for reference and from the information provided by the Bulgarian Government in response to the questions put by the Court that the action for damages, which is, in part, at the origin of the dispute in the main proceedings, is based on the Law on liability of the State and of municipalities for damage, referred to in paragraph 26 of this judgment, which establishes a system of State liability for harm caused by an infringement of the right to have a case examined and disposed of within a reasonable time, and that, in accordance with Article 7 of that law, it is the party whose unlawful acts, actions or omissions have caused the harm that is to be a party to the dispute and that, on that basis, is to stand in for the State from a procedural point of view.  
92      Thus, the role of the authority that caused the harm alleged in such an action for damages is different from that of the defendant in an action for indemnity by the State against the public official who is personally liable on account of shortcomings in the exercise of his or her office, since, in the latter case, that role seeks to defend private interests (see, to that effect, judgment of 18 May 2021,   
Asociaţia ‘Forumul Judecătorilor din România’ and Others  
, C-83/19, C-127/19, C-195/19, C-291/19, C-355/19 and C-397/19, EU:C:2021:393, paragraph 225).  
93      Therefore, in the light of the foregoing considerations, it should be considered that the processing, by the public prosecutor’s office of a Member State, of personal data initially collected and processed for one or more of the purposes set out in Article 1(1) of Directive 2016/680, for the purpose of defending the State in an action for damages for harm caused by misconduct on the part of that public prosecutor’s office in the performance of its tasks, is, in principle, liable to come not within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR but rather within that of point (e) of the first subparagraph of Article 6(1) of the GDPR.  
94      Moreover, it cannot be ruled out that, where, for the purpose of defending the State in an action for damages, the public prosecutor’s office of a Member State transmits personal data to the court having jurisdiction at that court’s request, that transmission is also liable to come within the scope of point (c) of the first subparagraph of Article 6(1) of the GDPR where, pursuant to the applicable national law, that public prosecutor’s office is required to comply with such a request.  
95      In those circumstances, for the purpose of establishing that processing of personal data such as that at issue in the main proceedings comes within the scope of the provisions of the first subparagraph of Article 6(1) of the GDPR, it is for the referring court to verify whether, in accordance with Article 6(3) of that regulation, the national law lays down, first, the basis for such processing and, second, the purposes of that processing or, as regards point (e) of the first subparagraph of Article 6(1) of that regulation, whether that processing is necessary for the public prosecutor’s office’s performance of its task carried out in the public interest.  
96      It is, moreover, for the referring court to determine whether the disclosure, by the public prosecutor’s office, of information concerning the person who has brought the action for damages, contained in files opened in cases other than that giving rise to that action, satisfies the other requirements laid down by the GDPR, and in particular the principle of ‘data minimisation’ referred to in Article 5(1)(c) of the GDPR, according to which personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and which gives expression to the principle of proportionality (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 98). In addition, it is for that court to verify that that processing of personal data has been carried out in compliance with the appropriate safeguards, in particular the possibility of effectively submitting comments on the information and evidence provided in that connection by the public prosecutor’s office, but also, in accordance with Article 21(1) of the GDPR, of objecting to the communication of that information and evidence to the court having jurisdiction, subject to the restrictions on that right of objection provided for by national legislation, in accordance with Article 23(1) of that regulation.  
97      In the light of all the foregoing, the answer to the second question is that:  
–        Article 3(8) and Article 9(1) and (2) of Directive 2016/680 and Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation is applicable to the processing of personal data by the public prosecutor’s office of a Member State for the purpose of exercising its rights of defence in an action for damages against the State, where, first, it informs the court having jurisdiction of the opening of files relating to a natural person who is a party to that action for the purposes set out in Article 1(1) of Directive 2016/680 and, second, it transmits those files to that court;  
–        Article 6(1) of the GDPR must be interpreted as meaning that, where an action for damages against the State is based on alleged misconduct on the part of the public prosecutor’s office in the performance of its tasks in criminal matters, such processing of personal data may be regarded as lawful if it is necessary for the performance of a task carried out in the public interest, within the meaning of point (e) of the first subparagraph of Article 6(1) of that regulation, for the purpose of defending the legal and financial interests of the State which falls to the public prosecutor’s office in those proceedings, provided that that processing of personal data complies with all the applicable requirements provided for by that regulation.  
   
Costs  
98      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Fifth Chamber) hereby rules:  
1.        
Article 1(1) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, read in conjunction with Article 4(2) and Article 6 thereof,  
must be interpreted as meaning that (i) the processing of personal data serves a purpose other than that for which those data were collected, where such data were collected for the purposes of the detection and investigation of a criminal offence, but that processing is carried out for the purpose of prosecuting a person following the conclusion of the criminal investigation at issue, irrespective of the fact that that person was considered to be a victim at the time of that collection, and that (ii) such processing is permitted pursuant to Article 4(2) of that directive, provided that it meets the conditions laid down in that provision.  
2.        
Article 3(8) and Article 9(1) and (2) of Directive 2016/680 and Article 2(1) and (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
must be interpreted as meaning that that regulation is applicable to the processing of personal data by the public prosecutor’s office of a Member State for the purpose of exercising its rights of defence in an action for damages against the State, where, first, it informs the court having jurisdiction of the opening of files relating to a natural person who is a party to that action for the purposes set out in Article 1(1) of Directive 2016/680 and, second, it transmits those files to that court.   
3.        
Article 6(1) of Regulation 2016/679  
must be interpreted as meaning that where an action for damages against the State is based on alleged misconduct on the part of the public prosecutor’s office in the performance of its tasks in criminal matters, such processing of personal data may be regarded as lawful if it is necessary for the performance of a task carried out in the public interest, within the meaning of point (e) of the first subparagraph of Article 6(1) of that regulation, for the purpose of defending the legal and financial interests of the State which falls to the public prosecutor’s office in those proceedings, provided that that processing of personal data complies with all the applicable requirements provided for by that regulation.

ID: 9669a770-f150-4240-95c3-d20b7a01513b

Judgment of 2 Oct 2018, C-207/16 (  
Ministerio Fiscal  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Confidentiality of electronic communications   
E-privacy Directive   
 >   
Electronic communications   
 >   
Data retention and access of national authorities   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
E-privacy Directive   
 >   
Material scope   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
   
JUDGMENT OF THE COURT (Grand Chamber)  
2 October 2018 (\*)  
(Reference for a preliminary ruling — Electronic communications — Processing of personal data — Directive 2002/58/EC — Articles 1 and 3 — Scope — Confidentiality of electronic communications — Protection — Article 5 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7 and 8 — Data processed in connection with the provision of electronic communications services — Access of national authorities to the data for the purposes of an investigation — Threshold of seriousness of an offence capable of justifying access to the data)  
In Case C-207/16,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain), made by decision of 6 April 2016, received at the Court on 14 April 2016, in the proceedings brought by  
Ministerio Fiscal,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Tizzano, Vice-President, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), J.L. da Cruz Vilaça, C.G. Fernlund and C. Vajda, Presidents of Chambers, E. Juhász, A. Borg Barthet, C. Toader, M. Safjan, D. Šváby, M. Berger, E. Jarašiūnas and E. Regan, Judges,  
Advocate General: H. Saugmandsgaard Øe,  
Registrar: L. Carrasco Marco, Administrator,  
having regard to the written procedure and further to the hearing on 29 January 2018,  
after considering the observations submitted on behalf of  
–        the Ministerio Fiscal, by E. Tejada de la Fuente,  
–        the Spanish Government, by M. Sampol Pucurull, acting as Agent,  
–        the Czech Government, by M. Smolek, J. Vláčil and A. Brabcová, acting as Agents,  
–        the Danish Government, by J. Nymann-Lindegren and M. Wolff, acting as Agents,  
–        the Estonian Government, by N. Grünberg, acting as Agent,  
–        Ireland, by M. Browne, L. Williams, E. Creedon and A. Joyce, acting as Agents, and by E. Gibson, Barrister-at-Law,  
–        the French Government, by D. Colas, E. de Moustier and E. Armoet, acting as Agents,  
–        the Latvian Government, by I. Kucina and J. Davidoviča, acting as Agents,  
–        the Hungarian Government, by M. Fehér and G. Koós, acting as Agents,  
–        the Austrian Government, by C. Pesendorfer, acting as Agent,  
–        the Polish Government, by B. Majczyna, D. Lutostańska and J. Sawicka, acting as Agents,  
–        the United Kingdom Government, by S. Brandon and C. Brodie, acting as Agents, and by C. Knight, Barrister, and G. Facenna QC,  
–        the European Commission, by I. Martínez del Peral, P. Costa de Oliveira, R. Troosters and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 3 May 2018,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns, in essence, the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings brought by the Ministerio Fiscal (Public Prosecutor’s Office, Spain) against the decision of the Juzgado de Instrucción No 3 de Tarragona (Court of Preliminary Investigation No 3, Tarragona, Spain, ‘the investigating magistrate’) refusing to grant the police access to personal data retained by providers of electronic communications services.  
   
Legal context  
   
EU law  
   
Directive 95/46  
3        According to Article 2(b) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), ‘processing of personal data’ means ‘any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction’.  
4        Article 3 of the directive, entitled ‘Scope’, provides as follows:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–      in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–      by a natural person in the course of a purely personal or household activity.’  
   
Directive 2002/58  
5        Recitals 2, 11, 15 and 21 of Directive 2002/58 state:  
‘(2)      This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the [Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.  
…  
(11)      Like Directive [95/46], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.  
…  
(15)      A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. …  
…  
(21)      Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.’  
6        Article 1 of Directive 2002/58, entitled ‘Scope and aim’, provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.  
2.      The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.  
3.      This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.’  
7        Article 2 of Directive 2002/58, entitled ‘Definitions’, is worded as follows:  
‘Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.  
The following definitions shall also apply:  
…  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  
(c)      “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
…’  
8        Article 3 of Directive 2002/58, entitled ‘Services concerned’, provides:  
‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.’  
9        Article 5 of Directive 2002/58, entitled ‘Confidentiality of the communications’, is worded as follows:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). …  
…  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. …’  
10      Article 6 of Directive 2002/58, entitled ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
…’  
11      Article 15 of that directive, entitled ‘Application of certain provisions of Directive [95/46]’, provides, in paragraph 1 thereof:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’  
   
Spanish law  
   
Law 25/2007  
12      Article 1 of Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (Law 25/2007 on the retention of data relating to electronic communications and to public communication networks) of 18 October 2007 (BOE No 251 of 19 October 2007, p. 42517) provides:  
‘1.      The purpose of this law is to regulate the obligation of operators to retain the data generated or processed in the context of the supply of electronic communications services or public communication networks, and the obligation to communicate those data to authorised agents whenever they are requested to do so by the necessary judicial authorisation, for the purposes of the detection, investigation and prosecution of serious offences provided for in the Criminal Code or in special criminal laws.  
2.      This law shall apply to traffic data and to location data concerning both natural and legal persons, and to related data necessary in order to identify the subscriber or registered user.  
…’  
   
The Criminal Code  
13      Article 13(1) of Ley Orgánica 10/1995 del Código Penal (Criminal Code) of 23 November 1995 (BOE No 281 of 24 November 1995, p. 33987) is worded as follows:  
‘Serious offences are those which the law punishes with a serious penalty.’  
14      Article 33 of the Criminal Code provides:  
‘1.      Depending on their nature and duration, penalties shall be classified as serious, less serious and light.  
2.      Serious penalties shall be:  
(a)      imprisonment for life, subject to review.  
(b)      imprisonment for a period of more than five years.  
…’  
   
Code of Criminal Procedure  
15      After the facts in the main proceedings had taken place, the Ley de Enjuiciamiento Criminal (Code of Criminal Procedure) was amended by Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (Organic Law 13/2015 amending the Code of Criminal Procedure in order to strengthen the procedural guarantees and regulate technological investigative measures) of 5 October 2015 (BOE No 239 of 6 October 2015, p. 90192).  
16      The law entered into force on 6 December 2015. It brings the field of access to telephone and telematic communications data which have been retained by providers of electronic communications services within the purview of the Code of Criminal Procedure.  
17      Article 579(1) of the Code of Criminal Procedure in the version as amended by Organic Law 13/2015 provides:  
‘1.      The court may authorise the interception of private postal and telegraphic correspondence, including fax, Burofax and international money orders, which the suspect sends or receives, and also the opening and analysis of such correspondence where there are grounds for thinking that that will permit the discovery or verification of a fact or a factor of relevance for the case, provided that the investigation relates to one of the following offences:  
(1)      Intentional offences punishable by a maximum penalty of at least three years’ imprisonment.  
(2)      Offences committed in the context of a criminal organisation.  
(3)      Terrorism offences.  
…’  
18      Article 588   
ter  
 j of the Code is worded as follows:  
‘1.      Electronic data retained by service providers or by persons who supply the communication pursuant to the legislation on the retention of electronic communications data, or on their own initiative for commercial or other reasons, and who are connected with communications processes, shall be communicated in order to be taken into account in the context of the proceedings only when authorised by the court.  
2.      Where knowledge of those data is essential for the investigation, application must be made to the competent court for authorisation to access the information in the automated archives of the service providers, in particular for the purpose of a cross search or a smart search of the data, provided that the nature of the data of which it is necessary to have knowledge and the reasons justifying the communication of those data are specified.’  
   
The main proceedings and the questions referred for a preliminary ruling  
19      Mr Hernandez Sierra lodged a complaint with the police for a robbery, which took place on 16 February 2015, during which he was injured and his wallet and mobile telephone were stolen.  
20      On 27 February 2015, the police requested the investigating magistrate to order various providers of electronic communications services to provide (i) the telephone numbers that had been activated between 16 February and 27 February 2015 with the International Mobile Equipment Identity code (‘the IMEI code’) of the stolen mobile telephone and (ii) the personal data relating to the identity of the owners or users of the telephone numbers corresponding to the SIM cards activated with the code, such as their surnames, forenames and, if need be, addresses.  
21      By order of 5 May 2015, the investigating magistrate refused that request. The latter held that the measure requested would not serve to identify the perpetrators of the offence. Moreover, it refused to grant the request on the ground that Law 25/2007 limited the communication of the data retained by the providers of electronic communications services to serious offences. Under the Criminal Code, serious offences are punishable by a term of imprisonment of more than five years, whereas the facts at issue in the main proceedings did not appear to constitute such an offence.  
22      The Public Prosecutor’s Office appealed against that order before the referring court, claiming that communication of the data at issue ought to have been allowed by reason of the nature of the facts and pursuant to a judgment of the Tribunal Supremo (Supreme Court, Spain) of 26 July 2010 relating to a similar case.  
23      The referring court explains that, subsequent to that order, the Spanish legislature amended the Code of Criminal Procedure by adopting Organic Law 13/2015. That legislation, which is relevant to the resolution of the case in the main proceedings, introduced two new alternative criteria for determining the degree of seriousness of an offence. The first is a substantive criterion, relating to conduct which corresponds to criminal classifications the criminal nature of which is specific and serious, and which is particularly harmful to individual and collective legal interests. Moreover, the national legislature relied on a formal normative criterion, based on the penalty prescribed for the offence in question. The threshold of three years’ imprisonment envisaged by that criterion does, however, cover the great majority of offences. In addition, the referring court considers that the State’s interest in punishing criminal conduct cannot justify disproportionate interferences with the fundamental rights enshrined in the Charter.  
24      In that regard, the referring court considers that, in the main proceedings, Directives 95/46 and 2002/58 establish a link with the Charter. The national legislation at issue in the main proceedings therefore comes within its scope, in accordance with Article 51(1) of the Charter, despite the fact that Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 (OJ 2006 L 105, p. 54) was annulled by the judgment of 8 April 2014,   
Digital Rights Ireland and Others  
 (C-293/12 and C-594/12, EU:C:2014:238).  
25      In that judgment, the Court recognised that the retention and communication of traffic data constitute particularly serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter and established criteria for the assessment of whether the principle of proportionality has been observed, including the seriousness of the offences warranting the retention of data and access thereto for the purposes of an investigation.  
26      In those circumstances, the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Can the sufficient seriousness of offences, as a criterion which justifies interference with the fundamental rights recognised by Articles 7 and 8 of the [Charter], be determined taking into account only the sentence which may be imposed in respect of the offence investigated, or is it also necessary to identify in the criminal conduct particular levels of harm to individual and/or collective legally protected interests?  
(2)      If it were in accordance with the constitutional principles of the European Union, used by the Court of Justice in its judgment [of 8 April 2014,   
Digital Rights Ireland and Others  
, C-293/12 and C-594/12, EU:C:2014:238] as standards for the strict review of [Directive 2002/58], to determine the seriousness of the offence solely on the basis of the sentence which may be imposed, what should the minimum threshold be? Would it be compatible with a general provision setting a minimum of three years’ imprisonment?’  
   
Procedure before the Court  
27      By decision of the President of the Court of 23 May 2016, the proceedings before the Court were stayed pending delivery of the judgment in   
Tele2 Sverige and Watson and Others  
, C-203/15 and C-698/15 (judgment of 21 December 2016, EU:C:2016:970, hereinafter ‘  
Tele2 Sverige and Watson and Others  
’). Further to the delivery of that judgment, the referring court was asked whether it wished to maintain or withdraw its request for a preliminary ruling. In its response by letter of 30 January 2017, received at the Court on 14 February 2017, the referring court stated that, in its view, that judgment did not enable it to assess with a sufficient degree of certainty the national legislation at issue in the main proceedings in the light of EU law. Consequently, the proceedings before the Court were resumed on 16 February 2017.  
   
Consideration of the questions referred  
28      The Spanish Government claims that, first, the Court lacks jurisdiction to reply to the request for a preliminary ruling and, secondly, the request is inadmissible.  
   
The jurisdiction of the Court  
29      In its written observations submitted to the Court, the Spanish Government expressed the view, endorsed by the United Kingdom Government during the hearing, that the Court does not have jurisdiction to answer the question referred for a preliminary ruling, on the ground that, in accordance with the first indent of Article 3(2) of Directive 95/46 and Article 1(3) of Directive 2002/58, the case in the main proceedings is excluded from the scope of those two directives. Therefore, the case does not fall within the scope of EU law, with the result that the Charter, in accordance with Article 51(1) thereof, is not applicable.  
30      According to the Spanish Government, the Court did, admittedly, rule in   
Tele2 Sverige and Watson and Others  
 that a legislative measure governing national authorities’ access to data retained by providers of electronic communications services comes within the scope of Directive 2002/58. However, the present case concerns a request for access made by a public authority, by virtue of a judicial decision in connection with a criminal investigation, to personal data retained by providers of electronic communications services. The Spanish Government infers that the request for access is part of national authorities’ exercise of   
jus puniendi  
, as a result of which it constitutes an activity of the State in areas of criminal law falling under the exception provided for in the first indent of Article 3(2) of Directive 95/46 and Article 1(3) of Directive 2002/58.  
31      In order to assess the claim that the Court does not have jurisdiction, it must be observed that Article 1(1) of Directive 2002/58 states that the directive provides for the harmonisation of the national provisions required, inter alia, to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector. In accordance with Article 1(2) thereof, the directive particularises and complements Directive 95/46 for the purposes set out in Article 1(1).  
32      Article 1(3) of Directive 2002/58 excludes from its scope ‘activities of the State’ in specified fields, including the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters (  
Tele2 Sverige and Watson and Others  
, paragraph 69 and the case-law cited). The activities mentioned therein by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (see, by analogy, in respect of the first indent of Article 3(2) of Directive 95/46, judgment of 10 July 2018,   
Jehovan Todistajat  
, C-25/17, EU:C:2018:551, paragraph 38 and the case-law cited).  
33      Article 3 of Directive 2002/58 states that the directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices (‘electronic communications services’). Consequently, that directive must be regarded as regulating the activities of the providers of such services (  
Tele2 Sverige and Watson and Others  
, paragraph 70).  
34      As regards Article 15(1) of Directive 2002/58, the Court has previously held that the legislative measures that are referred to in that provision come within the scope of that directive, even if they concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active, and even if the objectives that such measures must pursue overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of Directive 2002/58. Article 15(1) necessarily presupposes that the national measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met. Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services (see, to that effect,   
Tele2 Sverige and Watson and Others  
, paragraphs 72 to 74).  
35      The Court concluded that Article 15(1), read in conjunction with Article 3 of Directive 2002/58, must be interpreted as meaning that the scope of the directive extends not only to a legislative measure that requires providers of electronic communications services to retain traffic and location data, but also to a legislative measure relating to the access of the national authorities to the data retained by those providers (see, to that effect,   
Tele2 Sverige and Watson and Others  
, paragraphs 75 and 76).  
36      The protection of the confidentiality of electronic communications and related traffic data, guaranteed by Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including ‘any data related to such communications’, in order to protect the confidentiality of electronic communications (  
Tele2 Sverige and Watson and Others  
, paragraph 77).  
37      It should also be noted that legislative measures requiring providers of electronic communications services to retain personal data or to grant competent national authorities access to those data necessarily involve the processing, by those providers, of the data (see, to that effect,   
Tele2 Sverige and Watson and Others  
, paragraphs 75 and 78). Such measures, to the extent that they regulate the activities of such providers, cannot be regarded as activities characteristic of States, referred to in Article 1(3) of Directive 2002/58.  
38      In the present case, as stated in the order for reference, the request at issue in the main proceedings, by which the police seeks judicial authorisation to access personal data retained by providers of electronic communications services, is based on Law 25/2007, read in conjunction with the Code of Criminal Procedure in the version applicable to the facts in the main proceedings, which governs the access of public authorities to such data. That legislation permits the police, in the event that the judicial authorisation applied for on the basis of that legislation is granted, to require providers of electronic communications services to make personal data available to it and, in so doing, in the light of the definition in Article 2(b) of Directive 95/46, which is applicable in connection with Directive 2002/58 pursuant to the first paragraph of Article 2 of the latter directive, to ‘process’ those data within the meaning of the two directives. That legislation therefore governs the activities of providers of electronic communications services and, as a result, falls within the scope of Directive 2002/58.  
39      In those circumstances, the fact, noted by the Spanish Government, that the request for access was made in connection with a criminal investigation does not make Directive 2002/58 inapplicable to the case in the main proceedings by virtue of Article 1(3) of the directive.  
40      It is also irrelevant in that regard that the request for access at issue in the main proceedings relates, as is apparent from the Spanish Government’s written answer to a question raised by the Court and confirmed by both that government and the Public Prosecutor’s Office during the hearing, to the granting of access to only the telephone numbers corresponding to the SIM cards activated with the IMEI code of the stolen mobile telephone and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses, not to the data relating to the communications carried out with those SIM cards and the location data concerning the stolen mobile telephone.  
41      As observed by the Advocate General in point 54 of his Opinion, Directive 2002/58, pursuant to Article 1(1) and Article 3 thereof, governs all processing of personal data in connection with the provision of electronic communications services. In addition, in accordance with subparagraph (b) of the second paragraph of Article 2 of the directive, the notion of ‘traffic data’ covers ‘any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof’.  
42      In that connection, as regards, more specifically, data relating to the identity of owners of SIM cards, it is apparent from recital 15 of Directive 2002/58 that traffic data may include, inter alia, the name and address of the person sending a communication or using a connection to carry out a communication. Data relating to the identity of owners of SIM cards can also prove necessary in order to bill for the electronic communications services provided and therefore form part of traffic data as defined in subparagraph (b) of the second paragraph of Article 2 of the directive. Consequently, those data fall within the scope of Directive 2002/58.  
43      The Court therefore has jurisdiction to reply to the question raised by the referring court.  
   
Admissibility  
44      The Spanish Government argues that the request for a preliminary ruling is inadmissible on the ground that it does not clearly identify the provisions of EU law on which the Court is asked to give a preliminary ruling. What is more, the police request at issue in the main proceedings does not concern the interception of communications made by means of the SIM cards activated with the IMEI code of the stolen mobile telephone, but rather the establishment of a link between the cards and their owners, in such a way that the confidentiality of the communications is not affected. Article 7 of the Charter, referred to in the questions referred for a preliminary ruling, is therefore irrelevant to the present case.  
45      The Court has consistently held that it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions put by national courts concern the interpretation of a provision of EU law, the Court is, in principle, bound to give a ruling. The Court may refuse to rule on a question referred by a national court for a preliminary ruling only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 10 July 2018,   
Jehovan Todistajat  
, C-25/17, EU:C:2018:551, paragraph 31 and the case-law cited).  
46      In the present case, the order for reference contains sufficient factual and legal information required both for the definition of the provisions of EU law referred to in the questions referred for a preliminary ruling and for the understanding of the scope of those questions. More specifically, it is apparent from the order for reference that the questions referred for a preliminary ruling are intended to enable the referring court to assess whether, and to what extent, the national legislation, on which the police request at issue in the main proceedings is based, pursues an objective which is capable of justifying infringement of the fundamental rights enshrined in Articles 7 and 8 of the Charter. According to the statements of the referring court, that national legislation falls within the scope of Directive 2002/58, with the result that the Charter is applicable to the case in the main proceedings. The questions referred for a preliminary ruling are thus directly related to the subject matter of the main proceedings and cannot therefore be regarded as hypothetical.  
47      In those circumstances, the questions referred for a preliminary ruling are admissible.  
   
Substance  
48      By its two questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that public authorities’ access to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners of the SIM cards, entails interference with their fundamental rights, enshrined in those articles of the Charter, which is sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime and, if so, by reference to which criteria the seriousness of the offence at issue must be assessed.  
49      In that regard, it is apparent from the order for reference that, as observed in essence by the Advocate General in point 38 of his Opinion, the request for a preliminary ruling does not seek to determine whether the personal data at issue in the main proceedings have been retained by providers of electronic communications services in a manner consistent with the requirements laid down in Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter. As stated in paragraph 46 of this judgment, the request concerns only whether, and to what extent, the objective pursued by the legislation at issue in the main proceedings is capable of justifying the access of public authorities, such as the police, to such data, without the other conditions for access deriving from Article 15(1) forming part of the subject matter of the request.  
50      More specifically, the referring court is uncertain as to the factors that should be taken into consideration in order to assess whether the offences in respect of which the police may be authorised, for the purposes of an investigation, to have access to personal data retained by providers of electronic communications services are sufficiently serious to warrant the interference entailed by such access with the fundamental rights enshrined in Articles 7 and 8 of the Charter, as interpreted by the Court in its judgment of 8 April 2014,   
Digital Rights Ireland and Others  
 (C-293/12 and C-594/12, EU:C:2014:238), and in   
Tele2 Sverige and Watson and Others  
.  
51      As to the existence of an interference with those fundamental rights, it should be borne in mind, as observed by the Advocate General in points 76 and 77 of his Opinion, that the access of public authorities to such data constitutes an interference with the fundamental right to respect for private life, enshrined in Article 7 of the Charter, even in the absence of circumstances which would allow that interference to be defined as ‘serious’, without it being relevant that the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way. Such access also constitutes interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the Charter, as it constitutes processing of personal data (see, to that effect,   
Opinion 1/15 (EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, points 124 and 126 and the case-law cited).  
52      As regards the objectives that are capable of justifying national legislation, such as that at issue in the main proceedings, governing the access of public authorities to data retained by providers of electronic communications services and thereby derogating from the principle of confidentiality of electronic communications, it must be borne in mind that the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, as a result of which that access must correspond, genuinely and strictly, to one of those objectives (see, to that effect,   
Tele2 Sverige and Watson and Others  
, paragraphs 90 and 115).  
53      As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, it should be noted that the wording of the first sentence of Article 15(1) of Directive 2002/58 does not limit that objective to the fight against serious crime alone, but refers to ‘criminal offences’ generally.  
54      In that regard, the Court has admittedly held that, in areas of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying public authorities’ access to personal data retained by providers of electronic communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned (see, to that effect,   
Tele2 Sverige and Watson and Others  
, paragraph 99).  
55      However, the Court explained its interpretation by reference to the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails (see, to that effect,   
Tele2 Sverige and Watson and Others  
, paragraph 115).  
56      In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as ‘serious’.  
57      By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting ‘criminal offences’ generally.  
58      It should therefore, first of all, be determined whether, in the present case, in the light of the facts of the case, the interference with fundamental rights enshrined in Articles 7 and 8 of the Charter that police access to the data in question in the main proceedings would entail must be regarded as ‘serious’.  
59      In that regard, the sole purpose of the request at issue in the main proceedings, by which the police seeks, for the purposes of a criminal investigation, a court authorisation to access personal data retained by providers of electronic communications services, is to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile telephone. As noted in paragraph 40 of the present judgment, that request seeks access to only the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses. By contrast, those data do not concern, as confirmed by both the Spanish Government and the Public Prosecutor’s Office during the hearing, the communications carried out with the stolen mobile telephone or its location.  
60      It is therefore apparent that the data concerned by the request for access at issue in the main proceedings only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned.  
61      In those circumstances, access to only the data referred to in the request at issue in the main proceedings cannot be defined as ‘serious’ interference with the fundamental rights of the persons whose data is concerned.  
62      As stated in paragraphs 53 to 57 of this judgment, the interference that access to such data entails is therefore capable of being justified by the objective, to which the first sentence of Article 15(1) of Directive 2002/58 refers, of preventing, investigating, detecting and prosecuting ‘criminal offences’ generally, without it being necessary that those offences be defined as ‘serious’.  
63      In the light of the foregoing considerations, the answer to the questions referred is that Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights, enshrined in those articles of the Charter, which is not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime.  
   
Costs  
64      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights, enshrined in those articles of the Charter of Fundamental Rights, which is not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime.

ID: 97344e43-ea20-40b7-8943-6385311f94b8

Judgment of 9 Mar 2017, C-398/15 (  
Manni  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legal obligation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to object   
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
   
JUDGMENT OF THE COURT (Second Chamber)  
9 March 2017 (\*)  
(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Article 6(1)(e) — Data subject to disclosure in the companies register — First Directive 68/151/EEC — Article 3 — Winding-up of the company concerned — Restriction of access to that data by third parties)  
In Case C-398/15  
REQUEST for a preliminary ruling under Article 267 TFEU from the Corte suprema di cassazione (Court of Cassation, Italy), made by decision of 21 May 2015, received at the Court on 23 July 2015, in the proceedings  
Camera di Commercio,  
Industria, Artigianato e Agricoltura di Lecce  
v  
Salvatore Manni,  
THE COURT (Second Chamber),  
composed of M. Ilešič (Rapporteur), President of the Chamber, A. Prechal, A. Rosas, C. Toader and E. Jarašiūnas, Judges,  
Advocate General: Y. Bot,  
Registrar: I. Illéssy, Administrator,  
having regard to the written procedure and further to the hearing on 15 June 2016,  
after considering the observations submitted on behalf of:  
–        the Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce, by L. Caprioli, avvocato,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by E. De Bonis and P. Grasso, avvocati dello Stato,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the German Government, by T. Henze and J. Möller, acting as Agents,  
–        Ireland, by E. Creedon, J. Quaney and by A. Joyce, acting as Agents, and by A. Carroll, barrister,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes and M. Figueiredo and by C. Vieira Guerra, acting as Agents,  
–        the European Commission, by P. Costa de Oliveira and by D. Nardi and H. Støvlbæk, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 8 September 2016,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 3 of the First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community (OJ 1968 L 65, p. 8), as amended by Directive 2003/58/EC of the European Parliament and of the Council of 15 July 2003 (OJ 2003 L 221, p. 13) (‘Directive 68/151’), and Article 6(1)(e) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between the Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce (Chamber of Commerce, Industry, Crafts and Agriculture of Lecce, Italy, ‘the Chamber of Commerce of Lecce’) and Salvatore Manni concerning its refusal to delete certain personal data relating to Mr Manni from the companies register.  
   
Legal context  
   
EU law  
   
Directive 68/151  
3        As stated in recital 3 of Directive 2003/58, the aim of the directive was, inter alia, to modernise Directive 68/151 so as to make ‘company information more easily and rapidly accessible by interested parties, but should also simplify significantly the disclosure formalities imposed upon companies’.  
4        The recitals of Directive 68/151 are worded as follows:  
‘Whereas the co-ordination provided for in Article 54(3)(g) [of the EEC Treaty] and in the General Programme for the abolition of restrictions on freedom of establishment is a matter of urgency, especially in regard to companies limited by shares or otherwise having limited liability, since the activities of such companies often extend beyond the frontiers of national territories;  
Whereas the co-ordination of national provisions concerning disclosure, the validity of obligations entered into by, and the nullity of, such companies is of special importance, particularly for the purpose of protecting the interests of third parties;  
Whereas in these matters Community provisions must be adopted in respect of such companies simultaneously, since the only safeguards they offer to third parties are their assets;  
Whereas the basic documents of the company should be disclosed in order that third parties may be able to ascertain their contents and other information concerning the company, especially particulars of the persons who are authorised to bind the company;  
Whereas the protection of third parties must be ensured by provisions which restrict to the greatest possible extent the grounds on which obligations entered into in the name of the company are not valid;  
Whereas it is necessary, in order to ensure certainty in the law as regards relations between the company and third parties, and also between members, to limit the cases in which nullity can arise and the retroactive effect of a declaration of nullity, and to fix a short time limit within which third parties may enter objection to any such declaration’.  
5        Pursuant to Article 1 of Directive 68/151, the coordination measures prescribed by that directive apply to the laws, regulations and administrative provisions of the Member States relating to the forms of companies listed in that provision, including, for the Italian Republic, the   
società a responsabilità limitata  
 (limited liability company).  
6        Article 2 of that directive, which is set out in Section I thereof, entitled ‘Disclosure’, states:  
‘1.      Member States shall take the measures required to ensure compulsory disclosure by companies of at least the following documents and particulars:  
…  
(d)      the appointment, termination of office and particulars of the persons who either as a body constituted pursuant to law or as members of any such body:  
(i)      are authorized to represent the company in dealings with third parties and in legal proceedings;  
(ii)      take part in the administration, supervision or control of the company.  
…  
(h)      the winding-up of the company;  
…  
(j)      The appointment of liquidators, particulars concerning them, and their respective powers, unless such powers are expressly and exclusively derived from law or from the statutes of the company;  
(k)      the termination of the liquidation and, in Member States where striking off the register entails legal consequences, the fact of any such striking off.’  
7        Article 3 of that directive, which is also set out in that section, provides:  
‘1.      In each Member State a file shall be opened in a central register, commercial register or companies register, for each of the companies registered therein.  
2.      All documents and particulars which must be disclosed in pursuance of Article 2 shall be kept in the file or entered in the register; the subject matter of the entries in the register must in every case appear in the file.  
…  
3.      A copy of the whole or any part of the documents or particulars referred to in Article 2 must be obtainable on application. As from 1 January 2007 at the latest, applications may be submitted to the register by paper means or by electronic means as the applicant chooses.  
As from a date to be chosen by each Member State, which shall be no later than 1 January 2007, copies as referred to in the first subparagraph must be obtainable from the register by paper means or by electronic means as the applicant chooses. This shall apply in the case of all documents and particulars, irrespective of whether they were filed before or after the chosen date. However, Member States may decide that all, or certain types of, documents and particulars filed by paper means on or before a date which may not be later than 31 December 2006 shall not be obtainable from the register by electronic means if a specified period has elapsed between the date of filing and the date of the application submitted to the register. Such specified period may not be less than 10 years.  
…’  
8        Directive 68/151 was repealed and replaced by Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (OJ 2009 L 258, p. 11), as amended by Directive 2012/17/EU of the European Parliament and of the Council of 13 June 2012 (OJ 2012 L 156, p. 1).  
9        Directive 2012/17 introduced, inter alia, Article 7a into Directive 2009/101, which states:  
‘The processing of personal data carried out within the framework of this Directive shall be subject to Directive 95/46 ...’  
10      However, bearing in mind the date of the facts, the main proceedings are still governed by Directive 68/151.  
   
Directive 95/46  
11      Directive 95/46, the object of which, according to Article 1, is to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, and to remove obstacles to the free flow of personal data, states in recitals 10 and 25 thereof:  
‘(10)      Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;  
…  
(25)      Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons … responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances’.  
12      Article 2 of Directive 95/46 provides:  
‘For the purpose of this Directive:  
(a)      “personal data” mean any information relating to an identified or identifiable natural person (data subject), whereby an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;  
…’  
13      Article 3 of that directive, entitled ‘Scope’, states, in paragraph 1:  
‘This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.’  
14      In Section I (entitled ‘Principles relating to data quality’) of Chapter II of Directive 95/46, Article 6 is worded as follows:  
‘1.      Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes is not to be considered as incompatible provided that Member States provide appropriate safeguards.  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States must lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
15      In Section II (entitled ‘Criteria for making data processing legitimate’) of Chapter II of Directive 95/46, Article 7 provides:  
‘Member States shall provide that personal data may be processed only if:  
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;   
or  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;  
or  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
16      Article 12 of that directive, entitled ‘Rights of access’, provides:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
…  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
…’  
17      Article 14 of Directive 95/46, entitled ‘The data subject’s right to object’, provides:  
‘Member States shall grant the data subject the right:  
(a)      at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;  
…’  
18      Article 28 of Directive 95/46 provides for the establishment by the Member States of a supervisory authority responsible for supervising the application of the provisions adopted pursuant to that directive.  
   
Italian law  
19      Article 2188 of the codice civil (Civil Code) provides:  
‘A companies register shall be established for entries in the register required by law.  
The register shall be kept by the office of the companies register under the supervision of a judge appointed by the president of the court.  
The register shall be publicly available.’  
20      Article 8(1) and (2) of legge n. 580 — Riordinamento delle camere di commercio, industria, artigianato e agricoltura (Law No 580 on the reorganisation of the chambers of commerce, industry, craft trades and agriculture) of 29 December 1993 (Ordinary Supplement to GURI No 7 of 11 January 1994), provides that it is the responsibility of the chambers of commerce, industry, craft trades and agriculture to keep the register.  
21      Decreto del Presidente della Repubblica n. 581 — Regolamento di attuazione dell’articolo 8 della legge 29 dicembre 1993, n. 580, in materia di istituzione del registro delle imprese di cui all’articolo 2188 del codice civile (Decree No 581 of the President of the Republic, laying down implementing regulations for Article 8 of Law No 580, of 29 December 1993, concerning the establishment of the companies register referred to in Article 2188 of the Civil Code) of 7 December 1995 (GURI No 28 of 3 February 1996), governs certain details relating to the companies register.  
22      Directive 95/46 has been transposed into Italian law by decreto legislativo n. 196 — Codice in materia di protezione dei dati personali (Legislative Decree No 196 on the personal data protection code) of 30 June 2003 (Ordinary Supplement to GURI No 174 of 29 July 2003).  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
23      Mr Manni is the sole director of Italiana Costruzioni Srl, a building company which was awarded a contract for the construction of a tourist complex.  
24      By an action commenced on 12 December 2007, Mr Manni brought proceedings against the Lecce Chamber of Commerce, claiming that the properties in that complex were not selling because it was apparent from the companies register that he had been the sole director and liquidator of Immobiliare e Finanziaria Salentina Srl (‘Immobiliare Salentina’), which had been declared insolvent in 1992 and struck off the companies register, following liquidation proceedings, on 7 July 2005.  
25      In that action, Mr Manni alleged that the personal data concerning him, which appear in the companies register, had been processed by a company specialised in the collection and processing of market information and in risk assessment (‘rating’), and that, notwithstanding a request to remove it from the register, the Lecce Chamber of Commerce has not done so.  
26      Mr Manni therefore sought an order requiring the Lecce Chamber of Commerce to erase, anonymise or block the data linking him to the liquidation of Immobiliare Salentina, together with an order that that chamber compensate him for the damage he suffered by reason of the injury to his reputation.  
27      By judgment of 1 August 2011, the Tribunale di Lecce (Court of Lecce, Italy) upheld that claim, ordering the Lecce Chamber of Commerce to anonymise the data linking Mr Manni to the liquidation of Immobiliare Salentina and to pay compensation for the damage suffered by him, assessed at EUR 2 000, together with interest and costs.  
28      The Tribunale di Lecce (Court of Lecce) considered that ‘it is not permissible for entries in the register which link the name of an individual to a critical phase in the life of the company (such as its liquidation) to be permanent, unless there is a specific general interest in their retention and disclosure’. In the absence of any provision in the Civil Code laying down a maximum period of registration, that court held that, ‘after an appropriate period’ from the conclusion of the liquidation, and after the company has been removed from the register, stating the name of the person who was sole director of that company at the time of the liquidation ceased to be necessary and useful, for the purposes of Legislative Decree No 196, and the public interest in a ‘historical memory’ of the existence of the company and the difficulties it experienced [could] to a great extent be just as well effected by means of anonymous data’.  
29      The Lecce Chamber of Commerce brought an appeal against that judgment before the Corte suprema di cassazione (Court of Cassation, Italy), which decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must the principle of keeping personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed, laid down in Article 6(1)(e) of Directive 95/46, transposed by Legislative Decree No 196 of 30 June 2003, take precedence over and, therefore, preclude the system of disclosure established by means of the companies register provided for by Directive 68/151 and by national law in Article 2188 of the Civil Code and Article 8 of Law No 580 of 29 December 1993, in so far as it is a requirement of that system that anyone may, at any time, obtain the data relating to individuals in those registers?  
(2)      Consequently, is it permissible under Article 3 of Directive 68/151, by way of derogation from the principles that there should be no time limit and that anyone may consult the data published in the companies register, for the data no longer to be subject to “disclosure”, in both those regards, but to be available for only a limited period and only to certain recipients, on the basis of a case-by-case assessment by the data manager?’  
   
Consideration of the questions referred  
30      By its questions, which should be considered together, the referring court asks, essentially, whether Article 3 of Directive 68/151 and Article 6(1)(e) of Directive 95/46 must be interpreted as meaning that Member States may, and indeed must, allow individuals, covered by Article 2(1)(d) and (j) of Directive 68/151, to request the authority responsible for maintaining the companies register to limit, after a certain period has elapsed from the dissolution of the company concerned and on the basis of a case-by-case assessment, access to personal data concerning them and entered in that register.  
31      It should be noted at the outset that the case at issue in the main proceedings and the questions referred to the Court for a preliminary ruling do not concern the subsequent processing of the data at issue in this case by a specialised rating company, referred to in paragraph 25 of the present judgment, but rather the accessibility of such data held in the companies register by third parties.  
32      In that regard, it must first be pointed out that, under Article 2(1)(d) of Directive 68/151, Member States must take the measures necessary to ensure compulsory disclosure by companies of at least the appointment, termination of office and particulars of the persons who either as a body constituted pursuant to law, or as members of any such body, are authorised to represent the company in dealings with third parties and in legal proceedings, or take part in the administration, supervision or control of that company. Moreover, according to Article 2(1)(j), the appointment of liquidators, particulars concerning them and, in principle, their respective powers must also be disclosed.  
33      Pursuant to Article 3(1) to (3) of Directive 68/151, those particulars must be transcribed in each Member State either in a central register, commercial register or companies register (together, ‘the register’), and a copy of the whole or any part of those particulars must be obtainable by application.  
34      It must be held that the particulars concerning the identity of the persons referred to in Article 2(1)(d) and (j) of Directive 68/151 constitute, as information relating to identified or identifiable natural persons, ‘personal data’ within the meaning of Article 2(a) of Directive 95/46. It is apparent from the Court’s case-law that the fact that that information was provided as part of a professional activity does not mean that it cannot be characterised as personal data (see judgment of 16 July 2015,   
ClientEarth and PAN Europe  
 v   
EFSA  
, C-615/13 P, EU:C:2015:489, paragraph 30 and the case-law cited).  
35      Furthermore, by transcribing and keeping that information in the register and communicating it, where appropriate, on request to third parties, the authority responsible for maintaining that register carries out ‘processing of personal data’ for which it is the ‘controller’, within the meaning of the definitions set out Article 2(b) and (d) of Directive 95/46.  
36      The processing of personal data which is thus carried out in the implementation of Article 2(1)(d) and (j) and Article 3 of Directive 68/151 is subject to Directive 95/46, under Articles 1 and 3 thereof. This is now expressly provided for in Article 7a of Directive 2009/101, as amended by Directive 2012/17, which, however, is only declaratory in that regard. As the European Commission stated at the hearing, the EU legislature considered it useful to recall that fact in the context of the legislative changes introduced by Directive 2012/17 and aimed at ensuring interoperability of registers of the Member States, since those changes suggested an increase in the intensity of the processing of personal data.  
37      With regard to Directive 95/46, it should be remembered that, as is apparent from Article 1 and recital 10, that directive seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (see judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 66 and the case-law cited).  
38      According to recital 25 of Directive 95/46, the principles of protection laid down by the directive are reflected, on the one hand, in the obligations imposed on persons responsible for processing data, in particular regarding data quality, technical security, notification to the supervisory authority and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals whose data are the subject of processing to be informed that such processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.  
39      The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms and, in particular, the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union (‘the Charter’) (see judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 38 and the case-law cited).  
40      Article 7 of the Charter therefore guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data. Article 8(2) and (3) states that such data must be processed fairly, for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified, and that compliance with those rules is to be subject to control by an independent authority. Those requirements are implemented inter alia in Articles 6, 7, 12, 14 and 28 of Directive 95/46.  
41      With regard, in particular, to the general conditions of lawfulness imposed by Directive 95/46, it should be noted that, subject to the exceptions permitted under Article 13 of that directive, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (see, inter alia, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 71 and the case-law cited).  
42      In that regard, as the Advocate General pointed out in point 52 of his Opinion, it should be noted that the processing of personal data by the authority responsible for keeping the register pursuant to Article 2(1)(d) and (j) and Article 3 of Directive 68/151 satisfies several grounds for legitimation provided for in Article 7 of Directive 95/46, namely those set out in subparagraph (c) thereof, relating to compliance with a legal obligation, subparagraph (e), relating to the exercise of official authority or the performance of a task carried out in the public interest, and subparagraph (f) relating to the realisation of a legitimate interest pursued by the controller or by the third parties to whom the data are disclosed.  
43      With regard, inter alia, to the ground for legitimation provided for in Article 7(e) of Directive 95/46, it should be noted that the Court of Justice has already held that the activity of a public authority consisting in the storing, in a database, of data which undertakings are obliged to report on the basis of statutory obligations, permitting interested persons to search for that data and providing them with print-outs thereof, falls within the exercise of public powers (see judgment of 12 July 2012,   
Compass-Datenbank  
, C-138/11, EU:C:2012:449, paragraphs 40 and 41). Moreover, such an activity also constitutes a task carried out in the public interest within the meaning of that provision.  
44      In the present case, the parties to the main proceedings disagree as to whether the authority responsible for keeping the register should, after a certain period has elapsed since a company ceased to trade, and on the request of the data subject, either erase or anonymise that personal data, or limit their disclosure. In that context, the referring court asks in particular whether such an obligation flows from Article 6(1)(e) of Directive 95/46.  
45      According to Article 6(1)(e) of Directive 95/46, Member States are to ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Where that data are stored for longer periods for historical, statistical or scientific use, Member States must lay down appropriate safeguards. Pursuant to paragraph 2 of that article, it is the responsibility of the controller to ensure compliance with those principles.  
46      In the event of failure to comply with the condition laid down in Article 6(1)(e) of Directive 95/46, Member States guarantee the person concerned, pursuant to Article 12(b) thereof, the right to obtain from the controller, as appropriate, the erasure or blocking of the data concerned (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 70).  
47      Moreover, under subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, Member States are to grant the data subject the right, inter alia in the cases referred to in Article 7(e) and (f) of that directive, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. The balancing to be carried out under subparagraph (a) of the first paragraph of Article 14 thus enables account to be taken in a more specific manner of all the circumstances surrounding the data subject’s particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data (see judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 76).  
48      In order to determine whether Member States are required, under Article 6(1)(e) and Article 12(b), or under subsection (a) of the first subparagraph of Article 14 of Directive 95/46, to provide, for the natural persons referred to in Article 2(1)(d) and (j) of Directive 68/151, the right to apply to the authority responsible for keeping the register to erase or block the personal data entered in that register after a certain period of time, or to restrict access to it, it is first necessary to ascertain the purpose of that registration.  
49      In that regard, it is apparent from the recitals and from the title of Directive 68/151 that the purpose of the disclosure provided for by that directive is to protect in particular the interests of third parties in relation to joint stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets. To that end, the basic documents of the company concerned should be disclosed in order that third parties may be able to ascertain their contents and other information concerning the company, especially particulars of the persons who are authorised to bind the company.  
50      The Court has already noted, moreover, that the purpose of Directive 68/151 is to guarantee legal certainty in relation to dealings between companies and third parties in view of the intensification of trade between Member States following the creation of the internal market and that, with that in mind, it is important that any person wishing to establish and develop trading relations with companies situated in other Member States should be able easily to obtain essential information relating to the constitution of trading companies and to the powers of persons authorised to represent them, which requires that all the relevant information should be expressly stated in the register (see, to that effect, judgment of 12 November 1974,   
Haaga  
, 32/74, EU:C:1974:116, paragraph 6).  
51      Moreover, it is apparent from the case-law of the Court that the disclosure provided for in Article 3 of Directive 68/151 is intended to enable any interested third parties to inform themselves of these matters, without having to establish a right or an interest requiring to be protected. The Court noted, in that regard, that the very wording of Article 54(3)(g) of the EEC Treaty, on which that directive was based, refers to the need to protect the interests of third parties generally, without distinguishing or excluding any categories falling within the ambit of that term, and consequently the third parties referred to in that article cannot be limited in particular merely to creditors of the company concerned (see judgment of 4 December 1997,   
Daihatsu Deutschland  
, C-97/96, EU:C:1997:581, paragraphs 19, 20 and 22, and the order of 23 September 2004,   
Springer  
, C-435/02 and C-103/03, EU:C:2004:552, paragraphs 29 and 33).  
52      Furthermore, as to whether, in order to achieve the aim referred to in Article 3 of Directive 68/151, it is in principle necessary for the personal data of natural persons referred to in Article 2(1)(d) and (j) of that directive to remain on the register and/or accessible to any third party upon request also after the activity has ceased and the company concerned has been dissolved, it should be pointed out that the directive makes no express provision in that regard.  
53      However, as the Advocate General also pointed out in points 73 and 74 of his Opinion, it is common ground that even after the dissolution of a company, rights and legal relations relating to it continue to exist. Thus, in the event of a dispute, the data referred to in Article 2(1)(d) and (j) of Directive 68/151 may be necessary in order, inter alia, to assess the legality of an act carried out on behalf of that company during the period of its activity or so that third parties can bring an action against the members of the organs or against the liquidators of that company.  
54      Moreover, depending in particular on the limitation periods applicable in the various Member States, questions requiring such data may arise for many years after a company has ceased to exist.  
55      In view of the range of possible scenarios, which may involve actors in several Member States, and the considerable heterogeneity in the limitation periods provided for by the various national laws in the various areas of law, highlighted by the Commission, it seems impossible, at present, to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary.  
56      In those circumstances, Member States cannot, pursuant to Article 6(1)(e) and Article 12(b) of Directive 95/46, guarantee that the natural persons referred to in Article 2(1)(d) and (j) of Directive 68/151 have the right to obtain, as a matter of principle, after a certain period of time from the dissolution of the company concerned, the erasure of personal data concerning them, which have been entered in the register pursuant to the latter provision, or the blocking of that data from the public.  
57      That interpretation of Article 6(1)(e) and Article 12(b) of Directive 95/46 does not, moreover, result in disproportionate interference with the fundamental rights of the persons concerned, and particularly their right to respect for private life and their right to protection of personal data as guaranteed by Articles 7 and 8 of the Charter.  
58      First, Article 2(1)(d) and (j) and Article 3 of Directive 68/151 require disclosure only for a limited number of personal data items, namely those relating to the identity and the respective functions of persons having the power to bind the company concerned to third parties and to represent it or take part in the administration, supervision or control of that company, or having been appointed as liquidator of that company.  
59      Secondly, as pointed out in paragraph 49 of the present judgment, Directive 68/151 provides for disclosure of the data referred to in Article 2(1)(d) and (j) thereof, due, in particular, to the fact that the only safeguards that joint-stock companies and limited liability companies offer to third parties are their assets, which constitutes an increased economic risk for the latter. In view of this, it appears justified that natural persons who choose to participate in trade through such a company are required to disclose the data relating to their identity and functions within that company, especially since they are aware of that requirement when they decide to engage in such activity.  
60      Finally, as regards subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, it must be pointed out that, whereas it follows from the foregoing that, in the weighting to be carried out under that provision, in principle, the need to protect the interests of third parties in relation to joint-stock companies and limited liability companies and to ensure legal certainty, fair trading and thus the proper functioning of the internal market take precedence, it cannot be excluded, however, that there may be specific situations in which the overriding and legitimate reasons relating to the specific case of the person concerned justify exceptionally that access to personal data entered in the register is limited, upon expiry of a sufficiently long period after the dissolution of the company in question, to third parties who can demonstrate a specific interest in their consultation.  
61      In that regard, however, it should be pointed out that, in so far as the application of subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 is subject to the proviso that national law does not lay down a provision to the contrary, the final decision as to whether the natural persons referred to in Article 2(1)(d) and (j) of Directive 68/151 may apply to the authority responsible for keeping the register for such limitation of access to personal data concerning them, on the basis of a case-by-case assessment, is a matter for the national legislatures.  
62      It is for the referring court to determine the provisions of its national law in that regard.  
63      Assuming that such an examination reveals that national law permits such applications, it will be for the national court to assess, having regard to all the relevant circumstances and taking into account the time elapsed since the dissolution of the company concerned, the possible existence of legitimate and overriding reasons which, as the case may be, exceptionally justify limiting third parties’ access to the data concerning Mr Manni in the company register, from which it is apparent that he was the sole administrator and liquidator of Immobiliare Salentina. In that regard, it should be pointed out that the mere fact that, allegedly, the properties of a tourist complex built by Italiana Costruzioni, of which Mr Manni is currently the sole director, do not sell because of the fact that potential purchasers of those properties have access to that data in the company register, cannot be regarded as constituting such a reason, in particular in view of the legitimate interest of those purchasers in having that information.  
64      In the light of all the foregoing considerations, the answer to the questions referred must be that Article 6(1)(e), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, read in conjunction with Article 3 of Directive 68/151, must be interpreted as meaning that, as EU law currently stands, it is for the Member States to determine whether the natural persons referred to in Article 2(1)(d) and (j) of that directive may apply to the authority responsible for keeping the register to determine, on the basis of a case-by-case assessment, if it is exceptionally justified, on compelling legitimate grounds relating to their particular situation, to limit, on the expiry of a sufficiently long period after the dissolution of the company concerned, access to personal data relating to them, entered in that register, to third parties who can demonstrate a specific interest in consulting that data.  
   
Costs  
65      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
Article 6(1)(e), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, read in conjunction with Article 3 of the First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community, as amended by Directive 2003/58/EC of the European Parliament and of the Council of 15 July 2003, must be interpreted as meaning that, as EU law currently stands, it is for the Member States to determine whether the natural persons referred to in Article 2(1)(d) and (j) of that directive may apply to the authority responsible for keeping, respectively, the central register, commercial register or companies register to determine, on the basis of a case-by-case assessment, if it is exceptionally justified, on compelling legitimate grounds relating to their particular situation, to limit, on the expiry of a sufficiently long period after the dissolution of the company concerned, access to personal data relating to them, entered in that register, to third parties who can demonstrate a specific interest in consulting that data.

ID: 989bcd7f-26db-4539-83c7-8c5e3a8d24af

of 25 Jan 2024, C-687/21 (  
Saturn Electro  
)  
   
JUDGMENT OF THE COURT (Third Chamber)  
25 January 2024 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Interpretation of Articles 5, 24, 32 and 82 – Assessment of the validity of Article 82 – Inadmissibility of the request for an assessment of validity – Right to compensation for damage caused by data processing which infringes that regulation – Transmission of data to an unauthorised third party on account of an error made by the employees of the controller – Assessment of the appropriateness of the protective measures implemented by the controller – Compensatory function fulfilled by the right to compensation – Effect of the severity of the infringement – Whether necessary to establish the existence of damage caused by that infringement – Concept of ‘non-material damage’)  
In Case C-687/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Amtsgericht Hagen (Local Court, Hagen, Germany), made by decision of 11 October 2021, received at the Court on 16 November 2021, in the proceedings  
BL  
v  
MediaMarktSaturn Hagen-Iserlohn GmbH,   
formerly known as Saturn Electro-Handelsgesellschaft mbH Hagen,  
THE COURT (Third Chamber),  
composed of K. Jürimäe, President of the Chamber, N. Piçarra, M. Safjan, N. Jääskinen (Rapporteur) and M. Gavalec, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        BL, by D. Pudelko, Rechtsanwalt,  
–        MediaMarktSaturn Hagen-Iserlohn GmbH, formerly known as Saturn Electro-Handelsgesellschaft mbH Hagen, by B. Hackl, Rechtsanwalt,  
–        Ireland, by M. Browne, Chief State Solicitor, A. Joyce and M. Lane, acting as Agents, and by D. Fennelly, Barrister-at-Law,  
–        the European Parliament, by O. Hrstková Šolcová and J.-C. Puffer, acting as Agents,  
–        the European Commission, by A. Bouchagiar, M. Heller and H. Kranenborg, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2(1), Article 4, point 7, Article 5(1)(f), Article 6(1), Article 24, Article 32(1)(b) and (2), as well as Article 82 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’), and the assessment of the validity of Article 82.  
2        The request has been made in proceedings between BL, a natural person, and MediaMarktSaturn Hagen-Iserlohn GmbH, formerly known as Saturn Electro-Handelsgesellschaft mbH Hagen (‘Saturn’), concerning compensation for the non-material damage which that person claims to have suffered on account of the transmission by a third party of some of his personal data due to an error made by employees of that company.  
   
Legal context  
3        Recitals 11, 74, 76, 83, 85 and 146 of the GDPR are worded as follows:  
‘(11)      Effective protection of personal data throughout the [European] Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, …  
…  
(74)      The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.  
…  
(76)      The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.  
…  
(83)      In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.  
…  
(85)      A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. …  
…  
(146)      The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. …’  
4        In Chapter I of that regulation, relating to ‘general provisions’, Article 2 thereof, itself entitled ‘Material scope’, provides, in paragraph 1:  
‘This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.’  
5        Article 4 of that regulation, entitled ‘Definitions’, provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); …  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …  
…  
(10)      “third party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;  
…  
(12)      “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;  
…’  
6        Chapter II of the GDPR, entitled ‘Principles’, comprises Articles 5 to 11 of the regulation.  
7        Article 5 of that regulation, entitled ‘Principles relating to processing of personal data’, provides:  
‘1.      Personal data shall be:  
…  
(f)      processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
8        Article 6 of that regulation, entitled ‘Lawfulness of processing’, defines, in paragraph 1 thereof, the conditions that must be satisfied for processing to be lawful.  
9        Chapter IV of the GDPR, entitled ‘Controller and processor’, contains Articles 24 to 43 thereof.  
10      In Section 1 of Chapter IV entitled ‘General obligations’, that Article 24, itself entitled ‘Responsibility of the controller’, states, in paragraphs 1 and 2:  
‘1.      Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.  
2.      Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.’  
11      In Section 2 of Chapter IV entitled ‘Security of personal data’, Article 32 of the GDPR, itself entitled ‘Security of processing’, provides in paragraphs 1(b) and 2 thereof:  
‘1.      Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:  
…  
(b)      the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;  
…  
2.      In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.’  
12      Chapter VIII of the GDPR, entitled ‘Remedies, liability and penalties’, contains Articles 77 to 84 of that regulation.  
13      Under Article 82 of that regulation, entitled ‘Right to compensation and liability’:  
‘1.      Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.  
2.      Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. …  
3.      A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.  
…’  
14      Article 83 of the GDPR, entitled ‘General conditions for imposing administrative fines’, provides:  
‘1.      Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.’  
2.      … When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:  
(a)      the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;  
(b)      the intentional or negligent character of the infringement;  
…  
(d)      the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;  
…  
(k)      any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.  
3.      If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.  
…’  
15      Article 84 of that regulation, entitled ‘Penalties’, provides in paragraph 1 thereof:  
‘Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
16      The applicant in the main proceedings visited the commercial premises of Saturn, where he purchased an electrical household appliance. A sales contract and a credit agreement were drawn up, to that effect, by an employee of that company. At that same time, that employee entered in Saturn’s information system a number of items of personal data of that customer, namely his surname and first name, address, place of residence, name of his employer, income and bank details.  
17      The contractual documents containing that personal data were printed and signed by both parties. The applicant in the main proceedings then brought the documents to Saturn employees working at the collection counter. Another customer, who surreptitiously jumped the queue, accordingly received, by error, both the appliance ordered by the applicant in the main proceedings as well as the documents concerned and left with everything.  
18      As the error was quickly discovered, an employee of Saturn obtained the return of the appliance and the documents, then gave them to the applicant in the main proceedings, within half an hour after they had been given to the other customer. The undertaking wished to compensate the applicant in the main proceedings for that error by delivering the appliance concerned to the applicant’s home free of charge, but the applicant was of the view that that compensation was inadequate.  
19      The applicant in the main proceedings brought an action before the Amtsgericht Hagen (Local Court, Hagen, Germany), which is the referring court in the present case, seeking, in particular on the basis of the provisions of the GDPR, compensation for non-material damage that he claims to have suffered on account of the error made by the Saturn employees and the risk of a resulting loss of control over his personal data.  
20      In its defence, Saturn contends that there was not any infringement of the GDPR and that an infringement could only exist if it exceeded a certain threshold of severity, not reached in the present case. Furthermore, that company submits that the applicant in the main proceedings did not suffer any damage, since it was neither established nor put forward that the third party involved misused the personal data of the concerned party.  
21      The referring court questions, first, the validity of Article 82 of the GDPR, on account of that article appearing to it to lack detail as to its legal effects in the event of compensation for non-material damage.  
22      Secondly, if Article 82 is not declared invalid by the Court, the referring court asks whether exercising the right to compensation provided for in that article presupposes establishing the existence not only of an infringement of the GDPR but also damage, particularly non-material damage, suffered by the person seeking compensation.  
23      Thirdly, the referring court seeks to determine whether the mere fact that the printed documents containing personal data were transmitted without permission to a third party, on account of a mistake made by the employees of the controller, enables or does not enable a finding of infringement of the GDPR.  
24      Fourthly, while holding that ‘the [defendant] undertaking must bear the burden of proving its innocence’, that referring court seeks to know whether it suffices that such a negligent handover of documents took place, in order to hold that it amounts to an infringement of the GDPR, particularly regarding the obligation incumbent on the controller to implement appropriate measures to ensure the security of the processed data, under Articles 2, 5, 6 and 24 of that regulation.  
25      Fifthly, the referring court asks whether, even if it seems that the unauthorised third party was not aware of the personal data concerned before returning the documents containing those data, the existence of ‘non-material damage’, within the meaning of Article 82 of the GDPR, may be established from the mere fact that the person whose data were thus transmitted is fearful of the risk, which cannot be excluded according to that court, that those data are communicated to other individuals by that third party, and misused in the future.  
26      Sixthly, that referring court is seeking clarification as to the potential effect, in an action for non-material damage under Article 82, of the degree of severity of an infringement made in circumstances such as those in the main proceedings, given that more effective security measures could have been adopted, in its opinion, by the controller.  
27      Lastly, seventhly, the referring court seeks to ascertain the purpose of the compensation for non-material damage payable under the GDPR, by suggesting that that compensation could have the nature of a penalty equivalent to that of a contractual penalty.  
28      In those circumstances, the Amtsgericht Hagen (Local Court, Hagen) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      As no automatic legal effects are specified, is the compensation rule enacted in Article 82 of the [GDPR] invalid in the case of non-material damage?  
(2)      Is it necessary, for the purposes of the right to compensation, to establish the occurrence of non-material damage, to be demonstrated by the claimant, in addition to the unauthorised disclosure of the protected data to an unauthorised third party?  
(3)      Does the accidental disclosure of the personal data of the data subject (name, address, occupation, income, employer) to a third party in a paper document (printout), as the result of a mistake by employees of the [concerned] undertaking, suffice in order to establish infringement of the [GDPR]?  
(4)      Where the undertaking accidentally discloses, through its employees, data entered in an automated data processing system to an unauthorised third party in the form of a printout, does that accidental disclosure to a third party qualify as unlawful further processing (Article 2(1), Article 5(1)(f), Article 6(1) and Article 24 of the [GDPR])?  
(5)      Is non-material damage within the meaning of Article 82 of the [GDPR] incurred even where the third party who received the document containing the personal data did not read the data before returning the document containing the information, or does the discomfort of the person whose personal data were unlawfully disclosed suffice for the purpose of establishing non-material damage within the meaning of Article 82 of the [GDPR], given that every unauthorised disclosure of personal data entails the risk, which cannot be eliminated, that the data might nevertheless have been passed on to any number of people or even misused?  
(6)      Where accidental disclosure to third parties is preventable through better supervision of the undertaking’s helpers and/or better data security arrangements, for example by handling collections separately from contract documentation (especially financing documentation) under separate collection notes or by sending the documentation internally to the collection counter without giving the customer the printed documents and collection note, how serious should the infringement be considered to be (Article 32(1)(b) and (2) and Article 4, point 7, of the [GDPR])?  
(7)      Is compensation for non-material damage to be regarded as the award of a penalty similar to a contract penalty?’  
   
Consideration of the questions referred  
   
The first question  
29      By its first question, the referring court asks whether Article 82 of the GDPR is invalid in so far as it lacks detail as to the legal inferences which can be drawn by way of compensation for non-material damage.  
30      The European Parliament submits that that question is inadmissible, since the referring court did not meet the requirements of Article 94(c) of the Rules of Procedure of the Court of Justice, even if the referring court raises a particularly complex issue, namely the assessment of the validity of a provision of EU law.  
31      In accordance with Article 94(c) of the Rules of Procedure, the request for a preliminary ruling must, in particular, contain, in addition to the text of the questions referred to the Court for a preliminary ruling, a statement of the reasons which prompted the referring court or tribunal to inquire about the interpretation or validity of certain provisions of EU law.  
32      In that regard, the statement of the reasons for the reference for a preliminary ruling is necessary not only to enable the Court to give useful answers but also for the governments of the Member States and other interested parties to submit observations, in accordance with Article 23 of the Statute of the Court of Justice of the European Union. More specifically, it is in light of the grounds of invalidity set out in the referring decision that the Court must examine the validity of a provision of EU law, so that if there is no mention of the precise reasons which led the referring court to question the validity of that act or of those provisions, the questions relating to the invalidity thereof will be inadmissible (see, to that effect, judgments of 15 June 2017,   
T.KUP  
, C-349/16, EU:C:2017:469, paragraphs 16 to 18, and of 22 June 2023,   
Vitol  
, C-268/22, EU:C:2023:508, paragraphs 52 to 55).  
33      In the present case, however, the referring court does not put forward any specific information enabling the Court to examine the validity of Article 82 of the GDPR.  
34      Consequently, the first question must be declared inadmissible.  
   
The third and fourth questions  
35      By its third and fourth questions, which should be examined together and at the outset, the referring court asks, in essence, whether Articles 5, 24, 32 and 82 of the GDPR, read together, must be interpreted as meaning that, in an action for compensation under Article 82, the fact that the employees of the controller provided to an unauthorised third party in error a document containing personal data is sufficient, in itself, to consider that the technical and organisational measures implemented by the controller at issue were not ‘appropriate’, within the meaning of Articles 24 and 32.  
36      Article 24 of the GDPR lays down a general obligation, on the part of the controller of personal data, to implement appropriate technical and organisational measures to ensure that that processing is performed in accordance with that regulation and to be able to demonstrate this (judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraph 24).  
37      Article 32 of the GDPR sets out, for its part, the obligations of the controller and a possible processor as regards the security of that processing. Thus, paragraph 1 of that article provides that the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks in relation to that processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing concerned. Similarly, paragraph 2 of that article states that, in assessing the appropriate level of security, account is to be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (see, to that effect, judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraphs 26 and 27).  
38      It is apparent, accordingly, from the wording of Articles 24 and 32 of the GDPR that the appropriateness of the measures implemented by the controller must be assessed in a concrete manner, taking into account the various criteria referred to in those articles and the data protection needs specifically inherent in the processing concerned and the risks arising from the latter, and that all the more since that controller must be able to demonstrate that the measures it implemented comply with that regulation, a possibility which it would be deprived of if an irrebuttable presumption were accepted (see, to that effect, judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraphs 30 to 32).  
39      That literal interpretation is supported by reading Articles 24 and 32 together with Article 5(2) and Article 82 of that regulation, read in the light of recitals 74, 76 and 83 thereof, from which it follows, in particular, that the controller is obliged to mitigate the risks of personal data breaches and not prevent all breaches of those data (see, to that effect, judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraphs 33 to 38).  
40      Therefore, the Court interpreted Articles 24 and 32 of the GDPR as meaning that unauthorised disclosure of personal data or unauthorised access to those data by a ‘third party’, within the meaning of Article 4, point 10, of that regulation, are not sufficient, in themselves, for it to be held that the technical and organisational measures implemented by the controller in question were not ‘appropriate’, within the meaning of Articles 24 and 32 (judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraph 39).  
41      In the present case, the fact that the employees of the controller provided to an unauthorised third party in error a document containing personal data is capable of indicating that the technical and organisational measures implemented by the controller at issue were not ‘appropriate’, within the meaning of those Articles 24 and 32. In particular, such a circumstance may result from negligence or a failure in the controller’s organisation, which does not take into account in a concrete manner the risks in relation to the processing of the data at issue.  
42      In that regard, it must be pointed out that it follows from a reading of Articles 5, 24 and 32 of the GDPR together, read in the light of recital 74 thereof, that, in an action for compensation under Article 82 of that regulation, the controller concerned bears the burden of proving that the personal data are processed in such a way as to ensure appropriate security of those data, within the meaning of Article 5(1)(f) and of Article 32 of that regulation. Such an allocation of the burden of proof is capable not only of encouraging the controllers of those data of adopting the security measures required by the GDPR, but also in retaining the effectiveness of the right to compensation provided for in Article 82 of that regulation and upholding the intentions of the EU legislature referred to in recital 11 thereof (see, to that effect, judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraphs 49 to 56).  
43      Therefore, the Court interpreted the principle of accountability of the controller, set out in Article 5(2) of the GDPR and given expression in Article 24 thereof, as meaning that, in an action for compensation under Article 82 of that regulation, the controller in question bears the burden of proving that the security measures implemented by it are appropriate pursuant to Article 32 of that regulation (judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraph 57).  
44      Accordingly, a court hearing such an action for compensation under Article 82 of the GDPR cannot take into account only the fact that the employees of the controller provided to an unauthorised third party in error a document containing personal data, in order to determine whether there is an infringement of an obligation laid down in that regulation. That court must also take into account all of the evidence that the controller provided to demonstrate that the technical and organisational measures adopted by him or her are appropriate with a view to complying with his or her obligations under Articles 24 and 32 of that regulation.  
45      In light of the foregoing reasons, the answer to the third and fourth questions is that Articles 5, 24, 32 and 82 of the GDPR, read together, must be interpreted as meaning that, in an action for compensation based on Article 82, the fact that the employees of the controller provided to an unauthorised third party in error a document containing personal data is not sufficient, in itself, to consider that the technical and organisational measures implemented by the controller at issue were not ‘appropriate’, within the meaning of Articles 24 and 32.  
   
The seventh question  
46      By its seventh question, the referring court asks, in essence, whether Article 82 of the GDPR must be interpreted as meaning that the right to compensation provided for in that provision, in particular in the case of non-material damage, fulfils a punitive function.  
47      In that regard, the Court held that Article 82 of the GDPR fulfils a function that is compensatory and not punitive, contrary to other provisions of that regulation also contained in Chapter VIII thereof, namely Articles 83 and 84, which have, for their part, essentially a punitive purpose, since they permit the imposition of administrative fines and other penalties, respectively. The relationship between the rules set out in Article 82 and those set out in Articles 83 and 84 shows that there is a difference between those two categories of provisions, but also complementarity, in terms of encouraging compliance with the GDPR, it being observed that the right of any person to seek compensation for damage reinforces the operational nature of the protection rules laid down by that regulation and is likely to discourage the reoccurrence of unlawful conduct (see, to that effect, judgments of 4 May 2023,   
Österreichische Post (Non-material damage in connection with the processing of personal data)  
, C-300/21, EU:C:2023:370, paragraphs 38 and 40, and of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraph 85).  
48      The Court stated that, since the right to damages provided for in Article 82(1) of the GDPR does not fulfil a deterrent function, or even punitive, but fulfils a compensatory function, the severity of the infringement of that regulation that caused the damage concerned cannot influence the amount of the compensation granted under that provision, even where it concerns non-material damage and not material damage, in that that amount cannot exceed the full compensation for that damage (see, to that effect, judgment of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraphs 86 and 87).  
49      It follows from the foregoing that it is not necessary to rule on the alignment, contemplated by the referring court, between the purpose referred to by the right to compensation laid down in Article 82(1) and the punitive function of a contractual penalty.  
50      Therefore, the answer to the seventh question is that Article 82(1) of the GDPR must be interpreted as meaning that the right to compensation laid down in that provision, in particular in the case of non-material damage, fulfils a compensatory function, in that financial compensation based on that provision must allow the damage actually suffered as a result of the infringement of that regulation to be compensated in full, and not a punitive function.  
   
The sixth question  
51      By its sixth question, the referring court asks, in essence, whether Article 82 of the GDPR must be interpreted as meaning that that article requires that the degree of severity of the infringement of that regulation made by the controller is taken into consideration for the purposes of compensation under that provision.  
52      In that regard, it follows from Article 82 of the GDPR that, first, establishing the liability of the controller is, in particular, subject to fault on the part of the controller, which is presupposed unless it proves that it is not in any way responsible for the event giving rise to the damage, and secondly, Article 82 does not require that the severity of that fault is taken into consideration when setting the amount of the compensation allocated for non-material damage under that provision (judgment of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraph 103).  
53      As regards the assessment of the compensation payable under Article 82 of the GDPR, since that regulation does not contain a measure having such an aim, the national courts must, for the purpose of that assessment, apply the internal rules of each Member State relating to the extent of the pecuniary compensation, to the extent that the principles of equivalence and effectiveness of EU law can be observed (see, to that effect, judgment of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraphs 83 and 101 and the case-law cited).  
54      In addition, the Court stated that, having regard to the compensatory function of the right to compensation laid down in Article 82 of the GDPR, that provision does not require taking into consideration the severity of the infringement of that regulation, that the controller is presumed to have made, while setting the amount of the compensation allocated for non-material damage under that provision, but requires that that amount is set in a way that the damage actually suffered as a result of the infringement of that regulation is compensated in full (see, to that effect, judgment of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraphs 84 to 87 and 102 and the case-law cited).  
55      In light of the foregoing reasons, the answer to the sixth question that Article 82 of the GDPR must be interpreted as meaning that that article does not require that the severity of the infringement made by the controller be taken into consideration for the purposes of compensation under that provision.  
   
The second question  
56      By its second question, the referring court asks, in essence, whether Article 82(1) of the GDPR must be interpreted as meaning that the person seeking compensation under that provision is required to establish not only the infringement of provisions of that regulation, but also that that infringement led to his or her non-material or material damage.  
57      In that regard, it should be recalled that Article 82(1) of the GDPR provides that ‘any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered’.  
58      It is apparent from the wording of that provision that the mere infringement of the GDPR is not sufficient to confer a right to compensation. The existence of ‘damage’ or ‘harm’ which has been ‘suffered’ constitutes one of the conditions for the right to compensation laid down in Article 82(1), as does the existence of an infringement of that regulation and of a causal link between that damage and that infringement, those three conditions being cumulative (see, to that effect, judgments of 4 May 2023,   
Österreichische Post (Non-material damage in connection with the processing of personal data)  
, C-300/21, EU:C:2023:370, paragraphs 32 and 42; of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraph 77; of 14 December 2023,   
Gemeinde Ummendorf  
, C-456/22, EU:C:2023:988, paragraph 14; and of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraph 82).  
59      As regards, in particular, the non-material damage, the Court also held that Article 82(1) of the GDPR precludes a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject, as defined in Article 4, point 1, of that regulation, has reached a certain degree of seriousness (see, to that effect, judgments of 4 May 2023,   
Österreichische Post (Non-material damage in connection with the processing of personal data)  
, C-300/21, EU:C:2023:370, paragraph 51; of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraph 78; and of 14 December 2023,   
Gemeinde Ummendorf  
, C-456/78, EU:C:2023:988, paragraph 16).  
60      The Court stated that a person concerned by an infringement of the GDPR which had negative consequences for him or her is, however, required to demonstrate that those consequences constitute non-material damage, within the meaning of Article 82 of that regulation, since the mere infringement of the provisions thereof are not sufficient to confer a right to compensation (see, to that effect, judgments of 4 May 2023,   
Österreichische Post (Non-material damage in connection with the processing of personal data)  
, C-300/21, EU:C:2023:370, paragraphs 42 and 50; of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraph 84; and of 14 December 2023,   
Gemeinde Ummendorf  
, C-456/78, EU:C:2023:988, paragraphs 21 and 23).  
61      In light of the foregoing reasons, the answer to the second question is that Article 82(1) of the GDPR must be interpreted as meaning that the person seeking compensation by way of that provision is required to establish not only the infringement of provisions of that regulation, but also that that infringement caused him or her material or non-material damage.  
   
The fifth question  
62      By its fifth question, the referring court asks, in essence, whether Article 82(1) of the GDPR must be interpreted as meaning that, if a document containing personal data was provided to an unauthorised person, and it was established that that person did not become aware of those personal data, ‘non-material damage’, within the meaning of that provision, is likely to consist of the mere fact that the person concerned fears that, following that communication which made it possible to make a copy of that document before returning it, a dissemination, even abuse, of those data may occur in the future.  
63      It is important to specify that the referring court states that, in the present case, the document containing the data concerned was returned to the applicant in the main proceedings within half an hour following it having been provided to an unauthorised third party and that that unauthorised third party did not become aware of those data before the document’s return. That applicant submits, however, that that document’s provision gave that third party the possibility to take copies of the document before returning it and that it therefore created a fear for the applicant linked to the risk occurring in the future of those data being abused.  
64      Having regard to the absence of any reference in Article 82(1) of the GDPR to the domestic law of the Member States, the concept of ‘non-material damage’, within the meaning of that provision, must be given an autonomous and uniform definition specific to EU law (see, to that effect, judgments of 4 May 2023,   
Österreichische Post (Non-material damage in connection with the processing of personal data)  
, C-300/21, EU:C:2023:370, paragraphs 30 and 44, and of 14 December 2023,   
Gemeinde Ummendorf  
, C-456/22, EU:C:2023:988, paragraph 15).  
65      The Court held that it is apparent not only from the wording of Article 82(1) of the GDPR, read in the light of recitals 85 and 146 of that regulation, which encourage the acceptance of a broad interpretation of the concept of ‘non-material damage’ within the meaning of that first provision, but also the objective of ensuring a high level of protection of natural persons with regard to the processing of their personal data, which is referred to by the regulation, that the fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of that regulation is capable, in itself, of constituting ‘non-material damage’, within the meaning of Article 82(1) (see, to that effect, judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraphs 79 to 86).  
66      Furthermore, on the basis of considerations of a literal, systemic and teleological nature, the Court held that the loss of control of the personal data for a short period of time may cause the data subject ‘non-material damage’, within the meaning of Article 82(1) of the GDPR, giving rise to a right to compensation, subject to that person demonstrating having actually suffered such damage, however minimal, bearing in mind that the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation on that basis (see, to that effect, judgment of 14 December 2023,   
Gemeinde Ummendorf  
, C-456/22, EU:C:2023:988, paragraphs 18 to 23).  
67      Similarly, in the present case, it should be noted that it is consistent both with the wording of Article 82(1) of the GDPR and the objective of protection referred to by that regulation that the concept of ‘non-material damage’ encompasses a situation in which the data subject experiences the well-founded fear, which is for the national court to determine, that some of his or her personal data be subject to dissemination or misuse by third parties in the future, on account of the fact that a document containing those data was provided to an unauthorised third party who was afforded the opportunity to take copies before returning it.  
68      However, the fact remains that it is for the applicant in an action for compensation under Article 82 of the GDPR to demonstrate the existence of such damage. In particular, a purely hypothetical risk of misuse by an unauthorised third party cannot give rise to compensation. This is so where no third party became aware of the personal data at issue.  
69      Therefore, the answer to the fifth question is that Article 82(1) of the GDPR must be interpreted as meaning that, if a document containing personal data was provided to an unauthorised third party and it was established that that person did not become aware of those personal data, ‘non-material damage’, within the meaning of that provision, does not exist due to the mere fact that the data subject fears that, following that communication having made possible the making of a copy of that document before its recovery, a dissemination, even abuse, of those data may occur in the future.  
   
Costs  
70      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Articles 5, 24, 32 and 82 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), read together  
must be interpreted as meaning that in an action for compensation based on Article 82, the fact that the employees of the controller provided to an unauthorised third party in error a document containing personal data is not sufficient, in itself, to consider that the technical and organisational measures implemented by the controller at issue were not ‘appropriate’, within the meaning of Articles 24 and 32.  
2.        
Article 82(1) of Regulation 2016/679  
must be interpreted as meaning that the right to compensation laid down in that provision, in particular in the case of non-material damage, fulfils a compensatory function, in that financial compensation based on that provision must allow the damage actually suffered as a result of the infringement of that regulation to be compensated in full, and not a punitive function.  
3.        
Article 82 of Regulation 2016/679  
must be interpreted as meaning that that article does not require that the severity of the infringement made by the controller be taken into consideration for the purposes of compensation under that provision.  
4.        
Article 82(1) of Regulation 2016/679  
must be interpreted as meaning that the person seeking compensation by way of that provision is required to establish not only the infringement of provisions of that regulation, but also that that infringement caused him or her material or non-material damage.  
5.        
Article 82(1) of Regulation 2016/679  
must be interpreted as meaning that if a document containing personal data was provided to an unauthorised third party and it was established that that person did not become aware of those personal data, ‘non-material damage’, within the meaning of that provision, does not exist due to the mere fact that the data subject fears that, following that communication having made possible the making of a copy of that document before its recovery, a dissemination, even abuse, of those data may occur in the future.

ID: 9a5ec4d3-4c1f-464d-b3fb-f8d008e22dba

of 4 May 2023, C-300/21 (  
Österreichische Post  
)  
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Right to compensation and liability   
   
JUDGMENT OF THE COURT (Third Chamber)  
4 May 2023 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 82(1) – Right to compensation for damage caused by data processing that infringes that regulation – Conditions governing the right to compensation – Mere infringement of that regulation not sufficient – Need for damage caused by that infringement – Compensation for non-material damage resulting from such processing – Incompatibility of a national rule making compensation for such damage subject to the exceeding of a threshold of seriousness – Rules for the determination of damages by national courts)  
In Case C-300/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 15 April 2021, received at the Court on 12 May 2021, in the proceedings  
UI  
v  
Österreichische Post AG,  
THE COURT (Third Chamber),  
composed of K. Jürimäe, President of the Chamber, M. Safjan, N. Piçarra, N. Jääskinen (Rapporteur) and M. Gavalec, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
having considered the observations submitted on behalf of:  
–        UI, by himself as Rechtsanwalt,  
–        Österreichische Post AG, by R. Marko, Rechtsanwalt,  
–        the Austrian Government, by A. Posch, J. Schmoll and G. Kunnert, acting as Agents,  
–        the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
–        Ireland, by M. Browne, A. Joyce, M. Lane and M. Tierney, acting as Agents, and by D. Fennelly, Barrister-at-Law,  
–        the European Commission, by A. Bouchagiar, M. Heller and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 6 October 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 82 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’), read in conjunction with the principles of equivalence and effectiveness.  
2        The request has been made in proceedings between UI and Österreichische Post AG concerning the action brought by the former seeking compensation for the non-material damage which he claims to have suffered as a result of the processing by that company of data relating to the political affinities of persons resident in Austria, in particular himself, even though he had not consented to such processing.  
   
Legal context  
3        Recitals 10, 75, 85 and 146 of the GDPR are worded as follows:  
‘(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. …  
…  
(75)      The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, …  
…  
(85)      A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. …  
…  
(146)      The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in [EU] or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. …’  
4        Article 1 of the GDPR, headed ‘Subject matter and objectives’, provides in paragraphs 1 and 2:  
‘1.      This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.  
2.      This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.’  
5        Under Article 4(1) of that regulation, that article being entitled ‘Definitions’:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); …’  
6        Chapter VIII of the GDPR, entitled ‘Remedies, liability and penalties’, contains Articles 77 to 84 of that regulation.  
7        Article 77 of that regulation deals with the ‘right to lodge a complaint with a supervisory authority’, while Article 78 concerns the ‘right to an effective judicial remedy against a supervisory authority’.  
8        Article 82 of the GDPR, entitled ‘Right to compensation and liability’, states in paragraphs 1 and 2:  
‘1.      Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.  
2.      Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. …’  
9        Article 83 of that regulation, entitled ‘General conditions for imposing administrative fines’, provides in paragraph 1:  
‘Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.’  
10      Article 84(1) of that regulation, that article being headed ‘Penalties’, provides:  
‘Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
11      From 2017, Österreichische Post, a company incorporated under Austrian law, an address broker, collected information on the political affinities of the Austrian population. Using an algorithm that takes into account various social and demographic criteria, it defined ‘target group addresses’. The data thus generated were sold to various organisations, to enable them to send targeted advertising.  
12      In the course of its activity, Österreichische Post processed data which, by way of statistical extrapolation, led it to infer that the applicant in the main proceedings had a high degree of affinity with a certain Austrian political party. That information was not communicated to third parties, but the applicant in the main proceedings, who had not consented to the processing of his personal data, felt offended by the fact that an affinity with the party in question had been attributed to him. The fact that data relating to his supposed political opinions were retained within that company caused him great upset, a loss of confidence and a feeling of exposure. It is apparent from the order for reference that no harm other than those adverse emotional effects of a temporary nature has been established.  
13      In that context, the applicant in the main proceedings brought an action before the Landesgericht für Zivilrechtssachen Wien (Regional Court for Civil Matters, Vienna, Austria) seeking, first, an injunction for Österreichische Post to cease processing the personal data in question and, second, an order requiring that company to pay him the sum of EUR 1 000 by way of compensation for the non-material damage which he claims to have suffered. By decision of 14 July 2020, that court upheld the application for an injunction but rejected the claim for compensation.  
14      On appeal, the Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria) confirmed, by judgment of 9 December 2020, the decision at first instance. As regards the claim for compensation, that court referred to recitals 75, 85 and 146 of the GDPR and held that the Member States’ provisions of national law on civil liability supplement the provisions of that regulation, in so far as the latter does not contain special rules. In that regard, it noted that, under Austrian law, a breach of the rules on the protection of personal data is not automatically associated with non-material damage and gives rise to a right to compensation only where such damage reaches a certain ‘threshold of seriousness’. In its view, that is not the case with regard to the negative feelings which the applicant in the main proceedings has invoked.  
15      Hearing the action brought by the two parties in the main proceedings, the Oberster Gerichtshof (Supreme Court, Austria), by interim judgment of 15 April 2021, did not uphold the appeal on a point of law brought by Österreichische Post against the injunction imposed on it. Therefore, only the appeal on a point of law which the applicant in the main proceedings brought against the rejection of his claim for compensation which had been raised against him remains before that court.  
16      In support of its request for a preliminary ruling, the referring court states that it is apparent from recital 146 of the GDPR that Article 82 of that regulation established its own rules on liability for the protection of personal data, which superseded the rules in force in the Member States. Therefore, the concepts contained in Article 82, in particular the concept of ‘damage’ referred to in paragraph 1 thereof, should be interpreted autonomously and the conditions for the implementation of that liability should be defined in the light not of the rules of national law, but of the requirements of EU law.  
17      Specifically, in the first place, as regards the right to compensation for a breach of personal data protection, that court tends to consider, in the light of the sixth sentence of recital 146 of the GDPR, that compensation based on Article 82 of that regulation presupposes that material or non-material damage has actually been suffered by the data subject. It argues that the award of such compensation is subject to proof of specific damage distinct from that breach, which does not in itself establish the existence of non-material damage. In its view, recital 75 of that regulation refers to the mere possibility that non-material damage may result from the breaches listed therein and, although recital 85 refers to the risk of a ‘loss of control’ of the data affected, that risk is, however, uncertain in the present case, since those data were not transmitted to a third party.  
18      In the second place, as regards the assessment of the compensation that may be awarded under Article 82 of the GDPR, that court considers that the principle of effectiveness of EU law must have a limited impact, on the grounds that that regulation already provides for severe penalties for breaches thereof and that it is therefore not necessary to award a high level of compensation in addition to ensure its effectiveness. In its view, any compensation due on that basis must be proportionate, effective and dissuasive, so that the damages awarded may fulfil a compensatory function, but not be punitive in nature, which is extraneous to EU law.  
19      In the third place, the referring court questions the argument put forward by Österreichische Post that the award of such compensation is subject to the condition that the breach of personal data protection has caused particularly serious harm. In that regard, it notes that recital 146 of the GDPR advocates a broad interpretation of the concept of ‘damage’ within the meaning of that regulation. It takes the view that non-material damage must be compensated, under Article 82 of that regulation, if it is tangible, even if it is minor. By contrast, such damage should not be compensated if it appears to be completely negligible, as would be the case for the merely unpleasant feelings that are typically associated with such a breach.  
20      In those circumstances, the Oberster Gerichtshof (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Does the award of compensation under Article 82 of [the GDPR] also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?  
(2)      Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?  
(3)      Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence [or effect] of the infringement of at least some weight that goes beyond the upset caused by that infringement?’  
   
Consideration of the questions referred  
   
Whether Questions   
1 and 2 are admissible  
21      The applicant in the main proceedings submits, in essence, that the first question referred is inadmissible on the ground that it is hypothetical. He maintains, first of all, that his claim for compensation is not based on the ‘mere’ infringement of a provision of the GDPR. Next, the order for reference refers to the fact that there is agreement that compensation is due only if such infringement is accompanied by damage actually suffered. Finally, in his view, the only point that appears not to be common ground between the parties in the main proceedings is whether the damage must exceed a certain ‘threshold of seriousness’. If the Court were to answer the third question referred in that regard in the negative – as the applicant himself proposes – Question 1 would then be of no use for the resolution of that dispute.  
22      The applicant in the main proceedings also claims that the second question referred is inadmissible, on the ground that it is both very broad in content and too vague in wording, since the referring court refers to ‘EU-law requirements’, without specifying any such requirement.  
23      In that connection, it must be borne in mind that, according to settled case-law, it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court, which enjoy a presumption of relevance. If, therefore, the question referred concerns the interpretation or validity of a rule of EU law, the Court is, in principle, required to give a ruling, unless it is quite obvious that the interpretation sought bears no relation to the actual facts of the main action or to its purposes or where the problem is hypothetical or the Court does not have before it the factual or legal material necessary to give a useful answer to the question submitted to it (see, to that effect, judgments of 15 December 1995,   
Bosman  
, C-415/93, EU:C:1995:463, paragraph 61; of 7 September 1999,   
Beck and Bergdorf  
, C-355/97, EU:C:1999:391, paragraph 22; and of 5 May 2022,   
Zagrebačka banka  
, C-567/20, EU:C:2022:352, paragraph 43 and the case-law cited).  
24      In the present proceedings, Question 1 concerns the conditions required for the exercise of the right to compensation provided for in Article 82 of the GDPR. Furthermore, it is not obvious that the interpretation sought bears no relation to the dispute in the main action or that the problem raised is hypothetical. This dispute concerns a claim for compensation falling within the rules established by the GDPR for the protection of personal data. Moreover, that question seeks to determine whether, for the purposes of applying the rules on liability laid down by that regulation, it is necessary for the data subject to have suffered damage that is distinct from the infringement of that regulation.  
25      As regards Question 2, it has already been held that the mere fact that the Court is called upon to give a decision in abstract and general terms cannot have the effect of rendering a request for a preliminary ruling inadmissible (judgment of 15 November 2007,   
International Mail Spain  
, C-162/06, EU:C:2007:681, paragraph 24). A question submitted in such terms may be considered to be hypothetical, and therefore inadmissible, if the order for reference does not contain the minimum of explanatory material that would be necessary to establish a link between the question and the dispute in the main proceedings (see, to that effect, judgment of 8 July 2021,   
Sanresa  
, C-295/20, EU:C:2021:556, paragraphs 69 and 70).  
26      However, that is not the case here, since the referring court explains that Question 2 is based on a doubt as to whether, in the context of the assessment of the damages possibly owed by Österreichische Post due to a breach of the provisions of the GDPR, it is necessary to ensure compliance not only with the principles of equivalence and effectiveness, which are referred to in that question, but also with any other EU-law requirements. In that context, the absence of more precise information than that provided by that court concerning those principles does not deprive the Court of its ability to provide a useful interpretation of the relevant rules of EU law.  
27      Therefore, Questions 1 and 2 are admissible.  
   
Substance  
   
Question 1  
28      By Question 1 the referring court asks, in essence, whether Article 82(1) of the GDPR must be interpreted as meaning that the mere infringement of the provisions of that regulation is sufficient to confer a right to compensation.  
29      In that regard, it should be recalled that, according to settled case-law, the terms of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union (judgments of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 81, and of 10 February 2022,   
ShareWood Switzerland  
, C-595/20, EU:C:2022:86, paragraph 21), having regard, inter alia, to the wording of the provision concerned and to its context (see, to that effect, judgments of 15 April 2021,   
The North of England P & I Association  
, C-786/19, EU:C:2021:276, paragraph 48, and of 10 June 2021,   
KRONE   
–   
Verlag  
, C-65/20, EU:C:2021:471, paragraph 25).  
30      The GDPR makes no reference to the law of the Member States as regards the meaning and scope of the terms set out in Article 82 of that regulation, in particular as regards the concepts of ‘material or non-material damage’ and of ‘compensation for the damage suffered’. It follows that those terms must be regarded, for the purposes of the application of that regulation, as constituting autonomous concepts of EU law which must be interpreted in a uniform manner in all of the Member States.  
31      In the first place, as regards the wording of Article 82 of the GDPR, it should be recalled that paragraph 1 of that article states that ‘any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered’.  
32      It is clear from the wording of that provision that the existence of ‘damage’ which has been ‘suffered’ constitutes one of the conditions for the right to compensation laid down in that provision, as does the existence of an infringement of the GDPR and of a causal link between that damage and that infringement, those three conditions being cumulative.  
33      Therefore, it cannot be held that any ‘infringement’ of the provisions of the GDPR, by itself, confers that right to compensation on the data subject, as defined in Article 4(1) of that regulation. Such an interpretation would run counter to the wording of Article 82(1) of that regulation.  
34      Moreover, it is important to point out that the separate reference to ‘damage’ and to an ‘infringement’ in Article 82(1) of the GDPR would be superfluous if the EU legislature had considered that an infringement of the provisions of that regulation could be sufficient, by itself and in any event, to give rise to a right to compensation.  
35      In the second place, the foregoing literal interpretation is supported by the context of that provision.  
36      Article 82(2) of the GDPR, which specifies the rules on liability – the principle of which is established in paragraph 1 of that article – reproduces the three conditions necessary to give rise to the right to compensation, namely processing of personal data that infringes the provisions of the GDPR, damage suffered by the data subject, and a causal link between that unlawful processing and that damage.  
37      In addition, the clarifications provided by recitals 75, 85 and 146 of the GDPR support that interpretation. First, recital 146, which specifically concerns the right to compensation provided for in Article 82(1) of that regulation, refers, in its first sentence, to ‘damage which a person may suffer as a result of processing that infringes this Regulation’. Second, recitals 75 and 85 state, respectively, that ‘the risk … may result from personal data processing which could lead to … damage’ and that a ‘personal data breach may … result in … damage’. It follows, first, that the occurrence of damage in the context of such processing is only potential; second, that an infringement of the GDPR does not necessarily result in damage, and, third, that there must be a causal link between the infringement in question and the damage suffered by the data subject in order to establish a right to compensation.  
38      The literal interpretation of Article 82(1) of the GDPR is further supported by a comparison with other provisions also contained in Chapter VIII of that regulation, which governs, inter alia, the various remedies to protect the rights of the data subject in case of processing of his or her personal data that is allegedly contrary to the provisions of that regulation.  
39      In that regard, it should be noted that Articles 77 and 78 of the GDPR, contained in that chapter, provide for legal remedies before or against a supervisory authority, in case of an alleged infringement of that regulation, without it being stated that the data subject must have suffered ‘damage’ in order to be able to bring such actions, contrary to the wording of Article 82 of the GDPR with regard to actions for compensation. That difference in wording is indicative of the importance of the ‘damage’ criterion, and therefore of its distinctive nature as against the ‘infringement’ criterion, for the purposes of claims for compensation based on the GDPR.  
40      Similarly, Articles 83 and 84 of the GDPR, which permit the imposition of administrative fines and other penalties, have essentially a punitive purpose and are not conditional on the existence of individual damage. The relationship between the rules set out in Article 82 and those set out in Articles 83 and 84 shows that there is a difference between those two categories of provisions, but also complementarity, in terms of encouraging compliance with the GDPR, it being observed that the right of any person to seek compensation for damage reinforces the operational nature of the protection rules laid down by that regulation and is likely to discourage the reoccurrence of unlawful conduct.  
41      Last, it is important to note that the fourth sentence of recital 146 of the GDPR states that the rules laid down by the GDPR apply without prejudice to any claims for damages deriving from the violation of other rules of EU or Member State law.  
42      In the light of all of the foregoing reasons, the answer to Question 1 is that Article 82(1) of the GDPR must be interpreted as meaning that the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation.  
   
Question 3  
43      By Question 3, which it is appropriate to examine before Question 2, the referring court asks, in essence, whether Article 82(1) of the GDPR must be interpreted as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness.  
44      In that regard, it should be borne in mind that, as has been pointed out in paragraph 30 of the present judgment, the concept of ‘damage’ and, specifically in the present case, the concept of ‘non-material damage’, within the meaning of Article 82 of the GDPR, must be given an autonomous and uniform definition specific to EU law, in the absence of any reference to the domestic law of the Member States.  
45      In the first place, the GDPR does not define the concept of ‘damage’ for the purposes of the application of this instrument. Article 82 of that regulation confines itself to expressly stating that not only ‘material damage’ but also ‘non-material damage’ may give rise to a right to compensation, without any reference being made to any threshold of seriousness.  
46      In the second place, the context of that provision also tends to indicate that the right to compensation is not subject to the condition that the damage in question has reached a certain threshold of seriousness. The third sentence of recital 146 of the GDPR states that ‘the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation’. It would be contrary to that broad conception of ‘damage’, favoured by the EU legislature, if that concept were limited solely to damage of a certain degree of seriousness.  
47      In the third and last place, such an interpretation is supported by the objectives pursued by the GDPR. In that regard, it must be borne in mind that the third sentence of recital 146 of that regulation expressly calls for an interpretation of the concept of ‘damage’, within the meaning of the regulation, which ‘fully reflects the objectives of this Regulation’.  
48      It is apparent, in particular, from recital 10 of the GDPR that the objectives of the GDPR are, inter alia, to ensure a consistent and high level of protection of natural persons with regard to the processing of personal data within the European Union and, to that end, to ensure consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data throughout the European Union (see, to that effect, judgments of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 101, and of 12 January 2023,   
Österreichische Post (Information relating to the recipients of personal data)  
, C-154/21, EU:C:2023:3, paragraph 44 and the case-law cited).  
49      Making compensation for non-material damage subject to a certain threshold of seriousness would risk undermining the coherence of the rules established by the GDPR, since the graduation of such a threshold, on which the possibility or otherwise of obtaining that compensation would depend, would be liable to fluctuate according to the assessment of the courts seised.  
50      The fact remains that the interpretation thus adopted cannot be understood as meaning that a person concerned by an infringement of the GDPR which had negative consequences for him or her would be relieved of the need to demonstrate that those consequences constitute non-material damage within the meaning of Article 82 of that regulation.  
51      In the light of the foregoing reasons, the answer to Question 3 is that Article 82(1) of the GDPR must be interpreted as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness.  
   
Question 2  
52      By Question 2 the referring court asks, in essence, whether Article 82 of the GDPR must be interpreted as meaning that, for the purposes of determining the amount of damages payable under the right to compensation enshrined in that article, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, having due regard in particular to the principles of equivalence and effectiveness of EU law.  
53      In that connection, it should be recalled that, according to settled case-law, in the absence of EU rules on the matter, it is for the national legal order of each Member State to establish procedural rules for actions intended to safeguard the rights of individuals, in accordance with the principle of procedural autonomy, on condition, however, that those rules are not, in situations covered by EU law, less favourable than those governing similar domestic situations (principle of equivalence) and that they do not make it excessively difficult or impossible in practice to exercise the rights conferred by EU law (principle of effectiveness) (see, to that effect, judgments of 13 December 2017,   
El Hassani  
, C-403/16, EU:C:2017:960, paragraph 26, and of 15 September 2022,   
Uniqa Versicherungen  
, C-18/21, EU:C:2022:682, paragraph 36).  
54      In the present case, it should be noted that the GDPR does not contain any provision intended to define the rules on the assessment of the damages to which a data subject, within the meaning of Article 4(1) of that regulation, may be entitled under Article 82 thereof, where an infringement of that regulation has caused him or her harm. Therefore, in the absence of rules of EU law governing the matter, it is for the legal system of each Member State to prescribe the detailed rules governing actions for safeguarding rights which individuals derive from Article 82 and, in particular, the criteria for determining the extent of the compensation payable in that context, subject to compliance with those principles of equivalence and effectiveness (see, by analogy, judgment of 13 July 2006,   
Manfredi and Others  
, C-295/04 to C-298/04, EU:C:2006:461, paragraphs 92 and 98).  
55      As regards the principle of equivalence, in the present proceedings, the Court has nothing before it that is capable of raising doubts as to whether national legislation applicable to the dispute in the main proceedings complies with that principle and, therefore, of showing that that principle may have a specific effect in the context of that dispute.  
56      As regards the principle of effectiveness, it is for the referring court to determine whether the detailed rules laid down in Austrian law for the determination, by the courts, of damages due under the right to compensation enshrined in Article 82 of the GDPR, make it impossible in practice or excessively difficult to exercise the rights conferred by EU law, and more specifically by that regulation.  
57      In that context, it should be noted that the sixth sentence of recital 146 of the GDPR states that that instrument is intended to ensure ‘full and effective compensation for the damage they have suffered’.  
58      In that regard, in view of the compensatory function of the right to compensation under Article 82 of the GDPR, as the Advocate General pointed out, in essence, in points 39, 49 and 52 of his Opinion, financial compensation based on that provision must be regarded as ‘full and effective’ if it allows the damage actually suffered as a result of the infringement of that regulation to be compensated in its entirety, without there being any need, for the purposes of such compensation for the damage in its entirety, to require the payment of punitive damages.  
59      In the light of all of the foregoing considerations, the answer to Question 2 is that Article 82 of the GDPR must be interpreted as meaning that, for the purposes of determining the amount of damages payable under the right to compensation enshrined in that article, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are complied with.  
   
Costs  
60      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 82(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
must be interpreted as meaning that the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation.  
2.        
Article 82(1) of Regulation 2016/679  
must be interpreted as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness.  
3.        
Article 82 of Regulation 2016/679  
must be interpreted as meaning that for the purposes of determining the amount of damages payable under the right to compensation enshrined in that article, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are complied with.

ID: 9ace67a2-5cbd-4b0d-bdbc-311e6c3d8fc4

Judgment of 17 Oct 2013, C-291/12 (  
Schwarz  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Consent   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
   
JUDGMENT OF THE COURT (Fourth Chamber)  
17 October 2013 (\*)  
(Reference for a preliminary ruling – Area of freedom, security and justice – Biometric passport – Fingerprints – Regulation (EC) No 2252/2004 – Article 1(2) – Validity – Legal basis – Procedure for adopting – Articles 7 and 8 of the Charter of Fundamental Rights of the European Union – Right to respect for private life – Right to the protection of personal data – Proportionality)  
In Case C-291/12,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Gelsenkirchen (Germany), made by decision of 15 May 2012, received at the Court on 12 June 2012, in the proceedings  
Michael Schwarz  
v  
Stadt Bochum,  
THE COURT (Fourth Chamber),  
composed of L. Bay Larsen, President of the Chamber, M. Safjan, J. Malenovský (Rapporteur), U. Lõhmus and A. Prechal, Judges,  
Advocate General: P. Mengozzi,  
Registrar: K. Malacek, Administrator,  
having regard to the written procedure and further to the hearing on 13 March 2013,  
after considering the observations submitted on behalf of:  
–        Mr Schwarz, on his own behalf, and by W. Nešković, Rechtsanwalt,  
–        the Stadt Bochum, by S. Sondermann, acting as Agent,  
–        the German Government, by T. Henze and A. Wiedmann, acting as Agents,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the European Parliament, by U. Rösslein and P. Schonard, acting as Agents,  
–        the Council of the European Union, by I. Gurov and Z. Kupčová, acting as Agents,  
–        the European Commission, by B. Martenczuk and G. Wils, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 13 June 2013,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the validity of Article 1(2) of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ 2004 L 385, p. 1), as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009 (OJ 2009 L 142, p. 1; corrigendum: OJ 2009 L 188, p. 127) (‘Regulation No 2252/2004’).  
2        The request has been made in proceedings between Mr Schwarz and the Stadt Bochum (city of Bochum) concerning the latter’s refusal to issue him with a passport unless his fingerprints were taken at the same time so that they could be stored on that passport.  
   
Legal context   
3        Article 2 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) provides:  
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…’  
4        Article 7(e) of Directive 95/46 provides:  
‘Member States shall provide that personal data may be processed only if:  
…   
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed’.  
5        Recitals 2, 3 and 8 in the preamble to Regulation No 2252/2004 state:  
‘(2)      Minimum security standards for passports were introduced by a Resolution of the representatives of the Governments of the Member States, meeting within the Council, on 17 October 2000 [supplementing the resolutions of 23 June 1981, 30 June 1982, 14 July 1986 and 10 July 1995 as regards the security characteristics of passports and other travel documents (OJ 2000 C 310, p. 1)]. It is now appropriate to upgrade this Resolution by a Community measure in order to achieve enhanced harmonised security standards for passports and travel documents to protect against falsification. At the same time biometric identifiers should be integrated in the passport or travel document in order to establish a reliable link between the genuine holder and the document.  
(3)      The harmonisation of security features and the integration of biometric identifiers is an important step towards the use of new elements in the perspective of future developments at European level, which render the travel document more secure and establish a more reliable link between the holder and the passport and the travel document as an important contribution to ensuring that it is protected against fraudulent use. The specifications of the International Civil Aviation Organisation (ICAO), and in particular those set out in Document 9303 on machine readable travel documents, should be taken into account.  
…   
(8)      With regard to the personal data to be processed in the context of passports and travel documents, Directive [95/46] applies. It should be ensured that no further information shall be stored in the passport unless provided for in this Regulation, its annex or unless it is mentioned in the relevant travel document.’  
6        Under recital 5 in the preamble to Regulation No 444/2009:  
‘Regulation [No 2252/2004] requires biometric data to be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. This is without prejudice to any other use or storage of these data in accordance with national legislation of Member States. Regulation [No 2252/2004] does not provide a legal base for setting up or maintaining databases for storage of those data in Member States, which is strictly a matter of national law.’  
7        Under Article 1(1) to (2a) of Regulation No 2252/2004:  
‘1.      Passports and travel documents issued by Member States shall comply with the minimum security standards set out in the Annex.  
…  
2.      Passports and travel documents shall include a highly secure storage medium which shall contain a facial image. Member States shall also include two fingerprints taken flat in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.  
2a.      The following persons shall be exempt from the requirement to give fingerprints:  
(a)      Children under the age of 12 years.  
…   
(b)      persons, where fingerprinting is physically impossible.’  
8        Article 2(a) of that regulation provides:  
‘Additional technical specifications … for passports and travel documents relating to the following shall be established in accordance with the procedure referred to in Article 5(2):  
(a)      additional security features and requirements including enhanced anti-forgery, counterfeiting and falsification standards’.  
9        Article 3(1) of that regulation provides:   
‘In accordance with the procedure referred to in Article 5(2) it may be decided that the specifications referred to in Article 2 shall be secret and not be published. In that case, they shall be made available only to the bodies designated by the Member States as responsible for printing and to persons duly authorised by a Member State or the [European] Commission.’  
10      Under Article 4(3) of that regulation:   
‘Biometric data shall be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. For the purpose of this Regulation the biometric features in passports and travel documents shall only be used for verifying:  
(a)      the authenticity of the passport or travel document;  
(b)      the identity of the holder by means of directly available comparable features when the passport or travel document is required to be produced by law.  
The checking of the additional security features shall be carried out without prejudice to Article 7(2) of Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) [(OJ 2006 L 105, p. 1)]. The failure of the matching in itself shall not affect the validity of the passport or travel document for the purpose of the crossing of external borders.’  
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
11      Mr Schwarz applied to the Stadt Bochum for a passport, but refused at that time to have his fingerprints taken. After the Stadt Bochum rejected his application, Mr Schwarz brought an action before the referring court in which he requested that the city be ordered to issue him with a passport without taking his fingerprints.  
12      Before that court, Mr Schwarz disputes the validity of the regulation (Regulation No 2252/2004) which created the obligation to take the fingerprints of persons applying for passports. He submits that that regulation does not have an appropriate legal basis and is vitiated by a procedural defect. In addition, he claims that Article 1(2) of that regulation infringes the right to the protection of personal data laid down, in general terms, in Article 7 of the Charter of Fundamental Rights of the European Union (‘the Charter’), which relates to the right to respect for private life, and explicitly in Article 8 thereof.  
13      In those circumstances the Verwaltungsgericht Gelsenkirchen (Administrative Court, Gelsenkirchen) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
‘Is Article 1(2) of [Regulation No 2252/2004] to be considered valid?’  
   
Consideration of the question referred  
14      By its question, read in the light of the order for reference, the referring court asks, in essence, whether Article 1(2) of Regulation No 2252/2004 is invalid on the grounds, in the first place, that the regulation has an inappropriate legal basis; in the second, that the procedure for adopting that regulation is vitiated by a defect and, in the third, that Article 1(2) of that regulation breaches certain fundamental rights of the holders of passports issued in accordance with that provision.  
   
Legal basis of Regulation No 2252/2004  
15      The referring court seeks to establish whether it was permissible for the Council to adopt Regulation No 2252/2004 on the basis of Article 62(2)(a) EC, given that that provision does not explicitly refer to any power to regulate issues relating to passports and travel documents issued to citizens of the Union (‘passports’).  
16      In that regard, it should be noted that Article 62(2)(a) EC, in the version applicable from 1 May 1999 to 30 November 2009, on the basis of which Regulation No 2252/2004 was adopted, was part of Title IV of the EC Treaty, entitled ‘Visas, asylum, immigration and other policies related to free movement of persons’. That provision stated that the Council of the European Union, acting in accordance with the procedure referred to in Article 67 EC, was, within a period of five years after the entry into force of the Treaty of Amsterdam, to adopt ‘measures on the crossing of the external borders of the Member States which shall establish … standards and procedures to be followed by Member States in carrying out checks on persons at such borders’.  
17      It is clear from both the wording and the aim of Article 62(2)(a) EC that this provision authorised the Council to regulate how checks were to be carried out at the external borders of the European Union in order to ascertain the identity of persons crossing those borders. Such checks necessarily requiring documents to be presented that make it possible to establish that identity, Article 62(2)(a) EC therefore authorised the Council to adopt legal provisions relating to such documents and to passports in particular.  
18      As to whether Article 62(2)(a) EC authorised the Council to adopt measures establishing standards and procedures in connection with the issuing of passports to citizens of the Union, it should be noted, first, that the provision referred to checks on ‘persons’ without providing further details. Thus, it must be presumed that the provision was intended to cover not only third-country nationals, but also citizens of the Union and, hence, their passports.  
19      Second, as also confirmed by the Explanatory Memorandum to the proposal for a Council Regulation on standards for security features and biometrics in EU citizens’ passports [(COM(2004) 116 final)] as submitted by the Commission, harmonised security standards for passports may be required in order to avoid passports having security features which lag behind those provided for by the uniform format for visas and residence permits for third-country nationals. In those circumstances, the EU legislature has the authority to provide for similar security features in respect of passports held by EU citizens, in so far as such authority helps to prevent those passports from becoming targets for falsification or fraudulent use.  
20      It follows that Article 62(2)(a) EC was an appropriate legal basis for adopting Regulation No 2252/2004 and, in particular, Article 1(2) thereof.  
   
Procedure for adopting Regulation No 2252/2004  
21      The referring court seeks to establish whether Article 1(2) of Regulation No 2252/2004 is valid in view of the procedural requirements listed in Article 67(1) EC. In that regard, that court refers to the line of argument put forward by the applicant, who is of the view that, contrary to the requirements of the latter provision, the European Parliament was not properly consulted in the course of the legislative procedure. According to Mr Schwarz, the Commission’s proposal submitted to the Parliament for consultation purposes provided for the storage of images of fingerprints on passports to be merely an option for the Member States, changing into an obligation after the Parliament had been consulted. That represented a significant amendment; as a result, under Article 67 EC, further consultation of the Parliament was necessary.  
22      However, it is common ground that Regulation No 444/2009 has replaced the wording of Article 1(2) of Regulation No 2252/2004 – on the subject of which, according to the applicant, the Parliament was not consulted – with new wording which reproduces the obligation to store images of fingerprints in passports. Regulation No 444/2009 being applicable to the facts in the case before the referring court and adopted following the joint decision procedure and, so, with the full involvement of the Parliament in its role as co-legislator, the ground for invalidity relied on by the applicant in that regard is ineffective.  
   
Fundamental rights to respect for private life and the protection of personal data  
23      First, the Court must examine whether taking fingerprints and storing them in passports, as provided for in Article 1(2) of Regulation No 2252/2004, constitutes a threat to the rights to respect for private life and the protection of personal data. If so, it must then be ascertained whether such a threat can be justified.  
 Whether such a threat exists  
24      Article 7 of the Charter states, inter alia, that everyone has the right to respect for his or her private life. Under Article 8(1) thereof, everyone has the right to the protection of personal data concerning him or her.  
25      It follows from a joint reading of those articles that, as a general rule, any processing of personal data by a third party may constitute a threat to those rights.  
26      From the outset, it should be borne in mind that the right to respect for private life with regard to the processing of personal data concerns any information relating to an identified or identifiable individual (Joined Cases C-92/09 and C-93/09   
Volker und Markus Schecke and Eifert  
 [2010] ECR I-11063, paragraph 52, and Joined Cases C-468/10 and C-469/10   
ASNEF and FECEMD  
 [2011] ECR I-12181, paragraph 42).  
27      Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows those individuals to be identified with precision (see, to that effect, in particular, European Court of Human Rights judgment in   
S. and Marper v. United Kingdom  
, §§ 68 and 84, ECHR 2008).  
28      In addition, as can be seen from Article 2(b) of Directive 95/46, processing of personal data means any operation performed upon such data by a third party, such as the collecting, recording, storage, consultation or use thereof.  
29      Applying Article 1(2) of Regulation No 2252/2004 means that national authorities are to take a person’s fingerprints and that those fingerprints are to be kept in the storage medium in that person’s passport. Such measures must therefore be viewed as a processing of personal data.  
30      In those circumstances, the taking and storing of fingerprints by the national authorities which is governed by Article 1(2) of Regulation No 2252/2004 constitutes a threat to the rights to respect for private life and the protection of personal data. Accordingly, it must be ascertained whether that twofold threat is justified.  
 Justification  
31      Under Article 8(2) of the Charter, personal data cannot be processed except on the basis of the consent of the person concerned or some other legitimate basis laid down by law.  
32      First of all, concerning the condition requiring the consent of persons applying for passports before their fingerprints can be taken, it should be noted that, as a general rule, it is essential for citizens of the Union to own a passport in order, for example, to travel to non-member countries and that that document must contain fingerprints pursuant to Article 1(2) of Regulation No 2252/2004. Therefore, citizens of the Union wishing to make such journeys are not free to object to the processing of their fingerprints. In those circumstances, persons applying for passports cannot be deemed to have consented to that processing.  
33      Next, regarding whether the processing of fingerprints can be justified on the basis of some other legitimate basis laid down by law, it should be borne in mind from the outset that the rights recognised by Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect,   
Volker und Markus Schecke and Eifert  
, paragraph 48, and Case C-543/09   
Deutsche Telekom  
 [2011] ECR I-3441, paragraph 51).  
34      Indeed, Article 52(1) of the Charter allows for limitations of the exercise of those rights, so long as those limitations are provided for by law, respect the essence of those rights, and, in accordance with the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.  
35      First, in the present case, it is common ground that the limitation arising from the taking and storing of fingerprints when issuing passports must be considered to be provided for by law, for the purposes of Article 52(1) of the Charter, since those operations are provided for by Article 1(2) of Regulation No 2252/2004.  
36      Second, concerning the objective of general interest underlying that limitation, it can be seen that Article 1(2) of Regulation No 2252/2004, when read in the light of recitals 2 and 3 of that regulation, has two specific aims: the first, to prevent the falsification of passports and the second, to prevent fraudulent use thereof, that is to say, use by persons other than their genuine holders.  
37      Accordingly, Article 1(2) is designed, through pursuit of those aims, to prevent, inter alia, illegal entry into the European Union.  
38      In those circumstances, it must be found that Article 1(2) of Regulation No 2252/2004 pursues an objective of general interest recognised by the Union.  
39      Third, it is not apparent from the evidence available to the Court, nor has it been claimed, that the limitations placed on the exercise of the rights recognised by Articles 7 and 8 of the Charter in the present case do not respect the essence of those rights.  
40      Fourth, the Court must establish whether the limitations placed on those rights are proportionate to the aims pursued by Regulation No 2252/2004 and, by extension, to the objective of preventing illegal entry into the European Union. It must therefore be ascertained whether the measures implemented by that regulation are appropriate for attaining those aims and do not go beyond what is necessary to achieve them (see   
Volker und Markus Schecke and Eifert  
, paragraph 74).  
41      As to whether Article 1(2) of Regulation No 2252/2004 is appropriate for attaining the aim of preventing the falsification of passports, it is common ground that the storage of fingerprints on a highly secure storage medium as provided for by that provision requires sophisticated technology. Therefore such storage is likely to reduce the risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders.  
42      Mr Schwarz submits that the method of ascertaining identity using fingerprints is not appropriate for attaining the aim of preventing fraudulent use of passports, since there have been mistakes when implementing that method in practice; given that no two digital copies of a set of fingerprints are ever identical, systems using that method are not sufficiently accurate, resulting in not inconsiderable rates of unauthorised persons being incorrectly accepted and of authorised persons being incorrectly rejected.  
43      In that regard, however, it must be held that the fact that the method is not wholly reliable is not decisive. Although that method does not prevent all unauthorised persons from being accepted, it is enough that it significantly reduces the likelihood of such acceptance that would exist if that method were not used.  
44      Although it is true that the use of fingerprints as a means of ascertaining identity may, on an exceptional basis, lead to authorised persons being rejected by mistake, the fact remains that a mismatch between the fingerprints of the holder of a passport and the data in that document does not mean that the person concerned will automatically be refused entry to the European Union, as is pointed out in the second subparagraph of Article 4(3) of Regulation No 2252/2004. A mismatch of that kind will simply draw the competent authorities’ attention to the person concerned and will result in a more detailed check of that person in order definitively to establish his identity.  
45      In the light of the foregoing, the taking and storing of fingerprints referred to in Article 1(2) of Regulation No 2252/2004 are appropriate for attaining the aims pursued by that regulation and, by extension, the objective of preventing illegal entry to the European Union.  
46      Next, in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage measures which will interfere less with the rights recognised by Articles 7 and 8 of the Charter but will still contribute effectively to the objectives of the European Union rules in question (see, to that effect,   
Volker und Markus Schecke and Eifert  
, paragraph 86).  
47      In that context, with regard to the aim of protecting against the fraudulent use of passports, it must in the first place be considered whether the threat posed by the measure of taking fingerprints does not go beyond what is necessary in order to achieve that aim.  
48      In this respect, it is be borne in mind, on the one hand, that that action involves no more than the taking of prints of two fingers, which can, moreover, generally be seen by others, so that this is not an operation of an intimate nature. Nor does it cause any particular physical or mental discomfort to the person affected any more than when that person’s facial image is taken.  
49      It is true that those fingerprints are to be taken in addition to the facial image. However, the combination of two operations designed to identify persons may not   
a priori  
 be regarded as giving rise in itself to a greater threat to the rights recognised by Articles 7 and 8 of the Charter than if each of those two operations were to be considered in isolation.  
50      Thus, as regards the case in the main proceedings, nothing in the case file submitted to the Court permits a finding that the fact that fingerprints and a facial image are taken at the same time would, by reason of that fact alone, give rise to greater interference with those rights.  
51      On the other hand, it should also be noted that the only real alternative to the taking of fingerprints raised in the course of the proceedings before the Court is an iris scan. Nothing in the case file submitted to the Court suggests that the latter procedure would interfere less with the rights recognised by Articles 7 and 8 of the Charter than the taking of fingerprints.  
52      Furthermore, with regard to the effectiveness of those two methods, it is common ground that iris-recognition technology is not yet as advanced as fingerprint-recognition technology. In addition, the procedure for iris recognition is currently significantly more expensive than the procedure for comparing fingerprints and is, for that reason, less suitable for general use.  
53      In those circumstances, the Court has not been made aware of any measures which would be both sufficiently effective in helping to achieve the aim of protecting against the fraudulent use of passports and less of a threat to the rights recognised by Articles 7 and 8 of the Charter than the measures deriving from the method based on the use of fingerprints.  
54      In the second place, in order for Article 1(2) of Regulation No 2252/2004 to be justified in the light of that aim, it is also crucial that the processing of any fingerprints taken pursuant to that provision should not go beyond what is necessary to achieve that aim.  
55      In that regard, the legislature must ensure that there are specific guarantees that the processing of such data will be effectively protected from misuse and abuse (see, to that effect, European Court of Human Rights judgment,   
S. and Marper  
, § 103).  
56      In that respect, it should be noted that Article 4(3) of Regulation No 2252/2004 explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder.  
57      In addition, that regulation ensures protection against the risk of data including fingerprints being read by unauthorised persons. In that regard, Article 1(2) of that regulation makes it clear that such data are to be kept in a highly secure storage medium in the passport of the person concerned.  
58      However, the referring court is uncertain, in the light of its assessment, whether Article 1(2) of Regulation No 2252/2004 is proportionate in view of the risk that, once fingerprints have been taken pursuant to that provision, the – extremely high quality – data will be stored, perhaps centrally, and used for purposes other than those provided for by that regulation.  
59      In that regard, it is true that fingerprints play a particular role in the field of identifying persons in general. Thus, the identification techniques of comparing fingerprints taken in a particular place with those stored in a database make it possible to establish whether a certain person is in that particular place, whether in the context of a criminal investigation or in order to monitor that person indirectly.  
60      However, it should be borne in mind that Article 1(2) of Regulation No 2252/2004 does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone.  
61      The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself, as is pointed out by recital 5 of Regulation No 444/2009, be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the European Union.  
62      In those circumstances, the arguments put forward by the referring court concerning the risks linked to possible centralisation cannot, in any event, affect the validity of that regulation and would have, should the case arise, to be examined in the course of an action brought before the competent courts against legislation providing for a centralised fingerprint base.  
63      In the light of the foregoing, it must be held that Article 1(2) of Regulation No 2252/2004 does not imply any processing of fingerprints that would go beyond what is necessary in order to achieve the aim of protecting against the fraudulent use of passports.  
64      It follows that the interference arising from Article 1(2) of Regulation No 2252/2004 is justified by its aim of protecting against the fraudulent use of passports.  
65      In those circumstances, there is no longer any need to examine whether the measures put into effect by that regulation are necessary in view of its other aim (namely, preventing the falsification of passports).  
66      In the light of all the foregoing considerations, the answer to the question referred is that examination of that question has revealed nothing capable of affecting the validity of Article 1(2) of Regulation No 2252/2004.  
   
Costs  
67      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Fourth Chamber) hereby rules:  
Examination of the question referred has revealed nothing capable of affecting the validity of Article 1(2) of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009.

ID: 9d404155-51f1-45f9-b181-9516e92e559c

Judgment of 29 Jan 2008, C-275/06 (  
Promusicae  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Processing   
E-privacy Directive   
 >   
Electronic communications   
 >   
Confidentiality of electronic communications   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Data retention and access of national authorities   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
   
JUDGMENT OF THE COURT (Grand Chamber)  
29 January 2008 (\*)  
(Information society – Obligations of providers of services – Retention and disclosure of certain traffic data – Obligation of disclosure – Limits – Protection of the confidentiality of electronic communications – Compatibility with the protection of copyright and related rights – Right to effective protection of intellectual property)  
In Case C-275/06,  
REFERENCE for a preliminary ruling under Article 234 EC by the Juzgado de lo Mercantil No 5 de Madrid (Spain), made by decision of 13 June 2006, received at the Court on 26 June 2006, in the proceedings  
Productores de Música de España (Promusicae)  
v  
Telefónica de España SAU,  
THE COURT (Grand Chamber),  
composed of V. Skouris, President, C.W.A. Timmermans, A. Rosas, K. Lenaerts, G. Arestis and U. Lõhmus, Presidents of Chambers, A. Borg Barthet, M. Ilešič, J. Malenovský (Rapporteur), J. Klučka, E. Levits, A. Arabadjiev and C. Toader, Judges,  
Advocate General: J. Kokott,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 5 June 2007,  
after considering the observations submitted on behalf of:  
–        Productores de Música de España (Promusicae), by R. Bercovitz Rodríguez Cano, A. González Gozalo and J. de Torres Fueyo, abogados,  
–        Telefónica de España SAU, by M. Cornejo Barranco, procuradora, R. García Boto and P. Cerdán López, abogados,  
–        the Italian Government, by I.M. Braguglia, acting as Agent, assisted by S. Fiorentino, avvocato dello Stato,  
–        the Slovenian Government, by M. Remic and U. Steblovnik, acting as Agents,  
–        the Finnish Government, by J. Heliskoski and A. Guimaraes-Purokoski, acting as Agents,  
–        the United Kingdom Government, by Z. Bryanston-Cross, acting as Agent, and S. Malynicz, Barrister,  
–        the Commission of the European Communities, by R. Vidal Puig and C. Docksey, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 18 July 2007,  
gives the following  
Judgment  
1        This reference for a preliminary ruling concerns the interpretation of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) (OJ 2000 L 178, p. 1), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10), Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum, OJ 2004 L 195, p. 16), and Articles 17(2) and 47 of the Charter of Fundamental Rights of the European Union proclaimed in Nice on 7 December 2000 (OJ 2000 C 364, p. 1, ‘the Charter’).  
2        The reference was made in the course of proceedings between Productores de Música de España (Promusicae) (‘Promusicae’), a non-profit-making organisation, and Telefónica de España SAU (‘Telefónica’) concerning Telefónica’s refusal to disclose to Promusicae, acting on behalf of its members who are holders of intellectual property rights, personal data relating to use of the internet by means of connections provided by Telefónica.  
   
Legal context  
   
International law  
3        Part III of the Agreement on Trade-Related Aspects of Intellectual Property Rights (‘the TRIPs Agreement’), which constitutes Annex 1C to the Agreement establishing the World Trade Organisation (‘the WTO’), signed at Marrakesh on 15 April 1994 and approved by Council Decision 94/800/EC of 22 December 1994 concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994) (OJ 1994 L 336, p. 1), is headed ‘Enforcement of intellectual property rights’. That part includes Article 41(1) and (2), according to which:  
‘1.      Members shall ensure that enforcement procedures as specified in this Part are available under their law so as to permit effective action against any act of infringement of intellectual property rights covered by this Agreement, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements. These procedures shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.  
2.      Procedures concerning the enforcement of intellectual property rights shall be fair and equitable. They shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.’  
4        In Section 2 of Part III, ‘Civil and administrative procedures and remedies’, Article 42, headed ‘Fair and Equitable Procedures’, provides:  
‘Members shall make available to right holders civil judicial procedures concerning the enforcement of any intellectual property right covered by this Agreement …’  
5        Article 47 of the TRIPs Agreement, headed ‘Right of Information’, provides:  
‘Members may provide that the judicial authorities shall have the authority, unless this would be out of proportion to the seriousness of the infringement, to order the infringer to inform the right holder of the identity of third persons involved in the production and distribution of the infringing goods or services and of their channels of distribution.’  
   
Community law  
 Provisions relating to the information society and the protection of intellectual property, especially copyright  
–       Directive 2000/31  
6        Article 1 of Directive 2000/31 states:  
‘1.      This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.   
2.      This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.   
3.      This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.   
…  
5.      This Directive shall not apply to:  
…  
(b)      questions relating to information society services covered by Directives 95/46/EC and 97/66/EC;  
…’  
7        According to Article 15 of Directive 2000/31:  
‘1.      Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.   
2.      Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.’   
8        Article 18 of Directive 2000/31 provides:  
‘1.      Member States shall ensure that court actions available under national law concerning information society services’ activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.  
…’  
–       Directive 2001/29  
9        According to Article 1(1) of Directive 2001/29, the directive concerns the legal protection of copyright and related rights in the framework of the internal market, with particular emphasis on the information society.  
10      Under Article 8 of Directive 2001/29:  
‘1.      Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.   
2.      Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).   
3.      Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.’  
11      Article 9 of Directive 2001/29 reads:  
‘This Directive shall be without prejudice to provisions concerning in particular patent rights, trade marks, design rights, utility models, topographies of semi-conductor products, type faces, conditional access, access to cable of broadcasting services, protection of national treasures, legal deposit requirements, laws on restrictive practices and unfair competition, trade secrets, security, confidentiality, data protection and privacy, access to public documents, the law of contract.’  
–       Directive 2004/48  
12      Article 1 of Directive 2004/48 states:  
‘This Directive concerns the measures, procedures and remedies necessary to ensure the enforcement of intellectual property rights …’  
13      According to Article 2(3) of Directive 2004/48:  
‘3.      This Directive shall not affect:  
(a)      the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC, Directive 1999/93/EC or Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular;  
(b)      Member States’ international obligations and notably the TRIPS Agreement, including those relating to criminal procedures and penalties;  
(c)      any national provisions in Member States relating to criminal procedures or penalties in respect of infringement of intellectual property rights.’  
14      Article 3 of Directive 2004/48 provides:  
‘1.      Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.  
2.      Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.’  
15      Article 8 of Directive 2004/48 provides:  
‘1.      Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:  
(a)      was found in possession of the infringing goods on a commercial scale;  
(b)      was found to be using the infringing services on a commercial scale;  
(c)      was found to be providing on a commercial scale services used in infringing activities;  
or  
(d)      was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.  
2.      The information referred to in paragraph 1 shall, as appropriate, comprise:  
(a)      the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;  
(b)      information on the quantities produced, manufactured, delivered, received or ordered, as well as the price obtained for the goods or services in question.  
3.      Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which:  
(a)      grant the rightholder rights to receive fuller information;  
(b)      govern the use in civil or criminal proceedings of the information communicated pursuant to this Article;  
(c)      govern responsibility for misuse of the right of information;  
or  
(d)      afford an opportunity for refusing to provide information which would force the person referred to in paragraph 1 to admit to his/her own participation or that of his/her close relatives in an infringement of an intellectual property right;  
or  
(e)      govern the protection of confidentiality of information sources or the processing of personal data.’  
 Provisions on the protection of personal data  
–       Directive 95/46/EC  
16      Article 2 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) states:  
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…’  
17      According to Article 3 of Directive 95/46:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
…’  
18      Article 7 of Directive 95/46 reads as follows:  
‘Member States shall provide that personal data may be processed only if:  
…  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
19      Article 8 of Directive 95/46 provides:  
‘1.      Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.  
2.      Paragraph 1 shall not apply where:  
…  
(c)      processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent …  
…’  
20      According to Article 13 of Directive 95/46:  
‘1.      Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
(e)      an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;  
(f)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);  
(g)      the protection of the data subject or of the rights and freedoms of others.  
…’  
–       Directive 2002/58/EC  
21      Article 1 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37) states:  
‘1.      This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.  
2.      The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1 …  
3.      This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.’  
22      Under Article 2 of Directive 2002/58:  
‘Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) … shall apply.  
The following definitions shall also apply:  
…  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  
…  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
…’  
23      Article 3 of Directive 2002/58 provides:  
‘1.      This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.  
…’  
24      Article 5 of Directive 2002/58 provides:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
…’  
25      Article 6 of Directive 2002/58 provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
6.      Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.’  
26      Under Article 15 of Directive 2002/58:  
‘1.      Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.  
…’  
27      Article 19 of Directive 2002/58 provides:  
‘Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1).  
References made to the repealed Directive shall be construed as being made to this Directive.’  
   
National law  
28      Under Article 12 of Law 34/2002 on information society services and electronic commerce (Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico) of 11 July 2002 (BOE No 166 of 12 July 2002, p. 25388, ‘the LSSI’), headed ‘Duty to retain traffic data relating to electronic communications’:  
‘1.      Operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services must retain for a maximum of 12 months the connection and traffic data generated by the communications established during the supply of an information society service, under the conditions established in this article and the regulations implementing it.  
2.      … The operators of electronic communications networks and services and the service providers to which this article refers may not use the data retained for purposes other than those indicated in the paragraph below or other purposes permitted by the Law and must adopt appropriate security measures to avoid the loss or alteration of the data and unauthorised access to the data.  
3.      The data shall be retained for use in the context of a criminal investigation or to safeguard public security and national defence, and shall be made available to the courts or the public prosecutor at their request. Communication of the data to the forces of order shall be effected in accordance with the provisions of the rules on personal data protection.  
…’  
   
The main proceedings and the order for reference  
29      Promusicae is a non-profit-making organisation of producers and publishers of musical and audiovisual recordings. By letter of 28 November 2005 it made an application to the Juzgado de lo Mercantil No 5 de Madrid (Commercial Court No 5, Madrid) for preliminary measures against Telefónica, a commercial company whose activities include the provision of internet access services.  
30      Promusicae asked for Telefónica to be ordered to disclose the identities and physical addresses of certain persons whom it provided with internet access services, whose IP address and date and time of connection were known. According to Promusicae, those persons used the KaZaA file exchange program (peer-to-peer or P2P) and provided access in shared files of personal computers to phonograms in which the members of Promusicae held the exploitation rights.  
31      Promusicae claimed before the national court that the users of KaZaA were engaging in unfair competition and infringing intellectual property rights. It therefore sought disclosure of the above information in order to be able to bring civil proceedings against the persons concerned.  
32      By order of 21 December 2005 the Juzgado de lo Mercantil No 5 de Madrid ordered the preliminary measures requested by Promusicae.  
33      Telefónica appealed against that order, contending that under the LSSI the communication of the data sought by Promusicae is authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings or as a preliminary measure relating to civil proceedings. Promusicae submitted for its part that Article 12 of the LSSI must be interpreted in accordance with various provisions of Directives 2000/31, 2001/29 and 2004/48 and with Articles 17(2) and 47 of the Charter, provisions which do not allow Member States to limit solely to the purposes expressly mentioned in that law the obligation to communicate the data in question.  
34      In those circumstances the Juzgado de lo Mercantil No 5 de Madrid decided to stay the proceedings and refer the following question to the Court for a preliminary ruling:  
‘Does Community law, specifically Articles 15(2) and 18 of Directive [2000/31], Article 8(1) and (2) of Directive [2001/29], Article 8 of Directive [2004/48] and Articles 17(2) and 47 of the Charter … permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?’  
   
Admissibility of the question referred  
35      In its written observations the Italian Government submits that the statements in point 11 of the order for reference indicate that the question referred would be justified only in the event that the national legislation at issue in the main proceedings were interpreted as limiting the duty to disclose personal data to the field of criminal investigations or the protection of public safety and national defence. Since the national court does not exclude the possibility of that legislation being interpreted as not containing such a limitation, the question thus appears, according to the Italian Government, to be hypothetical, so that it is inadmissible.  
36      In this respect, it should be recalled that, in the context of the cooperation between the Court of Justice and the national courts provided for by Article 234 EC, it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine in the light of the particular circumstances of the case both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court (Case C-217/05   
Confederación Española de Empresarios de Estaciones de Servicio  
 [2006] ECR I-11987, paragraph 16 and the case-law cited).  
37      Where questions submitted by national courts concern the interpretation of a provision of Community law, the Court of Justice is thus bound, in principle, to give a ruling unless it is obvious that the request for a preliminary ruling is in reality designed to induce the Court to give a ruling by means of a fictitious dispute, or to deliver advisory opinions on general or hypothetical questions, or that the interpretation of Community law requested bears no relation to the actual facts of the main action or its purpose, or that the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see   
Confederación Española de Empresarios de Estaciones de Servicio  
, paragraph 17).  
38      Moreover, as regards the division of responsibilities under the cooperative arrangements established by Article 234 EC, the interpretation of provisions of national law is admittedly a matter for the national courts, not for the Court of Justice, and the Court has no jurisdiction, in proceedings brought on the basis of that article, to rule on the compatibility of national rules of law with Community law. On the other hand, the Court does have jurisdiction to provide the national court with all the guidance as to the interpretation of Community law necessary to enable that court to rule on the compatibility of national rules with Community law (see, to that effect, Case C-506/04   
Wilson  
 [2006] ECR I-8613, paragraphs 34 and 35, and Joined Cases C-338/04, C-359/04 and C-360/04   
Placanica and Others  
 [2007] ECR I-1891, paragraph 36).  
39      However, in the case of the present reference for a preliminary ruling, it is perfectly clear from the grounds of the order for reference as a whole that the national court considers that the interpretation of Article 12 of the LSSI depends on the compatibility of that provision with the relevant provisions of Community law, and hence on the interpretation of those provisions which it asks the Court to provide. Since the outcome of the main proceedings is thus linked to that interpretation, the question referred clearly does not appear hypothetical, so that the ground of inadmissibility put forward by the Italian Government cannot be accepted.  
40      The reference for a preliminary ruling is therefore admissible.  
   
The question referred for a preliminary ruling  
41      By its question the national court asks essentially whether Community law, in particular Directives 2000/31, 2001/29 and 2004/48, read also in the light of Articles 17 and 47 of the Charter, must be interpreted as requiring Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.  
   
Preliminary observations  
42      Even if, formally, the national court has limited its question to the interpretation of Directives 2000/31, 2001/29 and 2004/48 and the Charter, that circumstance does not prevent the Court from providing the national court with all the elements of interpretation of Community law which may be of use for deciding the case before it, whether or not that court has referred to them in the wording of its question (see Case C-392/05   
Alevizos  
 [2007] ECR I-3505, paragraph 64 and the case-law cited).  
43      It should be observed to begin with that the intention of the provisions of Community law thus referred to in the question is that the Member States should ensure, especially in the information society, effective protection of industrial property, in particular copyright, which Promusicae claims in the main proceedings. The national court proceeds, however, from the premiss that the Community law obligations required by that protection may be blocked, in national law, by the provisions of Article 12 of the LSSI.  
44      While that law, in 2002, transposed the provisions of Directive 2000/31 into domestic law, it is common ground that Article 12 of the law is intended to implement the rules for the protection of private life, which is also required by Community law under Directives 95/46 and 2002/58, the latter of which concerns the processing of personal data and the protection of privacy in the electronic communications sector, which is the sector at issue in the main proceedings.  
45      It is not disputed that the communication sought by Promusicae of the names and addresses of certain users of KaZaA involves the making available of personal data, that is, information relating to identified or identifiable natural persons, in accordance with the definition in Article 2(a) of Directive 95/46 (see, to that effect, Case C-101/01   
Lindqvist  
 [2003] ECR I-12971, paragraph 24). That communication of information which, as Promusicae submits and Telefónica does not contest, is stored by Telefónica constitutes the processing of personal data within the meaning of the first paragraph of Article 2 of Directive 2002/58, read in conjunction with Article 2(b) of Directive 95/46. It must therefore be accepted that that communication falls within the scope of Directive 2002/58, although the compliance of the data storage itself with the requirements of that directive is not at issue in the main proceedings.  
46      In those circumstances, it should first be ascertained whether Directive 2002/58 precludes the Member States from laying down, with a view to ensuring effective protection of copyright, an obligation to communicate personal data which will enable the copyright holder to bring civil proceedings based on the existence of that right. If that is not the case, it will then have to be ascertained whether it follows directly from the three directives expressly mentioned by the national court that the Member States are required to lay down such an obligation. Finally, if that is not the case either, in order to provide the national court with an answer of use to it, it will have to be examined, starting from the national court’s reference to the Charter, whether in a situation such as that at issue in the main proceedings other rules of Community law might require a different reading of those three directives.  
   
Directive 2002/58  
47      Article 5(1) of Directive 2002/58 provides that Member States must ensure the confidentiality of communications by means of a public communications network and publicly available electronic communications services, and of the related traffic data, and must inter alia prohibit, in principle, the storage of that data by persons other than users, without the consent of the users concerned. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and the technical storage necessary for conveyance of a communication. In addition, as regards traffic data, Article 6(1) of Directive 2002/58 provides that stored traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of that article and Article 15(1) of the directive.  
48      With respect, first, to paragraphs 2, 3 and 5 of Article 6, which relate to the processing of traffic data in accordance with the requirements of billing and marketing services and the provision of value added services, those provisions do not concern the communication of that data to persons other than those acting under the authority of the providers of public communications networks and publicly available electronic communications services. As to the provisions of Article 6(6) of Directive 2002/58, they do not relate to disputes other than those between suppliers and users concerning the grounds for storing data in connection with the activities referred to in the other provisions of that article. Since Article 6(6) thus clearly does not concern a situation such as that of Promusicae in the main proceedings, it cannot be taken into account in assessing that situation.  
49      With respect, second, to Article 15(1) of Directive 2002/58, it should be recalled that under that provision the Member States may adopt legislative measures to restrict the scope inter alia of the obligation to ensure the confidentiality of traffic data, where such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, as referred to in Article 13(1) of Directive 95/46.  
50      Article 15(1) of Directive 2002/58 thus gives Member States the possibility of providing for exceptions to the obligation of principle, imposed on them by Article 5 of that directive, to ensure the confidentiality of personal data.  
51      However, none of these exceptions appears to relate to situations that call for the bringing of civil proceedings. They concern, first, national security, defence and public security, which constitute activities of the State or of State authorities unrelated to the fields of activity of individuals (see, to that effect,   
Lindqvist  
, paragraph 43), and, second, the prosecution of criminal offences.  
52      As regards the exception relating to unauthorised use of the electronic communications system, this appears to concern use which calls into question the actual integrity or security of the system, such as the cases referred to in Article 5(1) of Directive 2002/58 of the interception or surveillance of communications without the consent of the users concerned. Such use, which, under that article, makes it necessary for the Member States to intervene, also does not relate to situations that may give rise to civil proceedings.  
53      It is clear, however, that Article 15(1) of Directive 2002/58 ends the list of the above exceptions with an express reference to Article 13(1) of Directive 95/46. That provision also authorises the Member States to adopt legislative measures to restrict the obligation of confidentiality of personal data where that restriction is necessary inter alia for the protection of the rights and freedoms of others. As they do not specify the rights and freedoms concerned, those provisions of Article 15(1) of Directive 2002/58 must be interpreted as expressing the Community legislature’s intention not to exclude from their scope the protection of the right to property or situations in which authors seek to obtain that protection in civil proceedings.  
54      The conclusion must therefore be that Directive 2002/58 does not preclude the possibility for the Member States of laying down an obligation to disclose personal data in the context of civil proceedings.  
55      However, the wording of Article 15(1) of that directive cannot be interpreted as compelling the Member States, in the situations it sets out, to lay down such an obligation.  
56      It must therefore be ascertained whether the three directives mentioned by the national court require those States to lay down that obligation in order to ensure the effective protection of copyright.  
   
The three directives mentioned by the national court  
57      It should first be noted that, as pointed out in paragraph 43 above, the purpose of the directives mentioned by the national court is that the Member States should ensure, especially in the information society, effective protection of industrial property, in particular copyright. However, it follows from Article 1(5)(b) of Directive 2000/31, Article 9 of Directive 2001/29 and Article 8(3)(e) of Directive 2004/48 that such protection cannot affect the requirements of the protection of personal data.  
58      Article 8(1) of Directive 2004/48 admittedly requires Member States to ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided. However, it does not follow from those provisions, which must be read in conjunction with those of paragraph 3(e) of that article, that they require the Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.  
59      Nor does the wording of Articles 15(2) and 18 of Directive 2000/31 or that of Article 8(1) and (2) of Directive 2001/29 require the Member States to lay down such an obligation.  
60      As to Articles 41, 42 and 47 of the TRIPs Agreement, relied on by Promusicae, in the light of which Community law must as far as possible be interpreted where – as in the case of the provisions relied on in the context of the present reference for a preliminary ruling – it regulates a field to which that agreement applies (see, to that effect, Joined Cases C-300/98 and C-392/98   
Dior and Others  
 [2000] ECR I-11307, paragraph 47, and Case C-431/05   
Merck Genéricos – Produtos Farmacêuticos  
 [2007] ECR I-0000, paragraph 35), while they require the effective protection of intellectual property rights and the institution of judicial remedies for their enforcement, they do not contain provisions which require those directives to be interpreted as compelling the Member States to lay down an obligation to communicate personal data in the context of civil proceedings.  
   
Fundamental rights  
61      The national court refers in its order for reference to Articles 17 and 47 of the Charter, the first of which concerns the protection of the right to property, including intellectual property, and the second of which concerns the right to an effective remedy. By so doing, that court must be regarded as seeking to know whether an interpretation of those directives to the effect that the Member States are not obliged to lay down, in order to ensure the effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings leads to an infringement of the fundamental right to property and the fundamental right to effective judicial protection.  
62      It should be recalled that the fundamental right to property, which includes intellectual property rights such as copyright (see, to that effect, Case C-479/04   
Laserdisken  
 [2006] ECR I-8089, paragraph 65), and the fundamental right to effective judicial protection constitute general principles of Community law (see respectively, to that effect, Joined Cases C-154/04 and C-155/04   
Alliance for Natural Health and Others  
 [2005] ECR I-6451, paragraph 126 and the case-law cited, and Case C-432/05   
Unibet  
 [2007] ECR I-2271, paragraph 37 and the case-law cited).  
63      However, the situation in respect of which the national court puts that question involves, in addition to those two rights, a further fundamental right, namely the right that guarantees protection of personal data and hence of private life.  
64      According to recital 2 in the preamble to Directive 2002/58, the directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter. In particular, the directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter. Article 7 substantially reproduces Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950, which guarantees the right to respect for private life, and Article 8 of the Charter expressly proclaims the right to protection of personal data.  
65      The present reference for a preliminary ruling thus raises the question of the need to reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other.  
66      The mechanisms allowing those different rights and interests to be balanced are contained, first, in Directive 2002/58 itself, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for, and in the three directives mentioned by the national court, which reserve the cases in which the measures adopted to protect the rights they regulate affect the protection of personal data. Second, they result from the adoption by the Member States of national provisions transposing those directives and their application by the national authorities (see, to that effect, with reference to Directive 95/46,   
Lindqvist  
, paragraph 82).  
67      As to those directives, their provisions are relatively general, since they have to be applied to a large number of different situations which may arise in any of the Member States. They therefore logically include rules which leave the Member States with the necessary discretion to define transposition measures which may be adapted to the various situations possible (see, to that effect,   
Lindqvist  
, paragraph 84).  
68      That being so, the Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality (see, to that effect,   
Lindqvist  
, paragraph 87, and Case C-305/05   
Ordre des barreaux francophones et germanophone and Others  
 [2007] ECR I-0000, paragraph 28).  
69      Moreover, it should be recalled here that the Community legislature expressly required, in accordance with Article 15(1) of Directive 2002/58, that the measures referred to in that paragraph be adopted by the Member States in compliance with the general principles of Community law, including those mentioned in Article 6(1) and (2) EU.  
70      In the light of all the foregoing, the answer to the national court’s question must be that Directives 2000/31, 2001/29, 2004/48 and 2002/58 do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.  
   
Costs  
71      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

ID: 9df58a09-b908-487c-83da-334c0035ad78

of 30 Mar 2023, C-34/21 (  
Hauptpersonalrat der Lehrerinnen und Lehrer  
)  
General data protection law   
 >   
Chapter IX - Provisions relating to specific processing operations   
 >   
Processing in the context of employment   
General data protection law   
 >   
Chapter IX - Provisions relating to specific processing operations   
 >   
Processing in the context of employment   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legal obligation   
   
JUDGMENT OF THE COURT (First Chamber)  
30 March 2023 (\*)  
(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 88(1) and (2) – Processing of data in the employment context – Regional school system – Teaching by videoconference as a result of the COVID-19 pandemic – Implementation without the express consent of the teachers)  
In Case C-34/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), made by decision of 20 December 2020, received at the Court on 20 January 2021, in the proceedings  
Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium  
v  
Minister des Hessischen Kultusministeriums,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, K. Lenaerts, President of the Court, L. Bay Larsen, Vice-President of the Court, acting as Judges of the First Chamber, A. Kumin and I. Ziemele (Rapporteur), Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: S. Beer, Administrator,  
having regard to the written procedure and further to the hearing on 30 June 2022,  
after considering the observations submitted on behalf of:  
–        the Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium, by J. Kolter, Rechtsanwalt,  
–        the Minister des Hessischen Kultusministeriums, by C. Meinert,  
–        the German Government, by J. Möller and D. Klebs, acting as Agents,  
–        the Austrian Government, by G. Kunnert and J. Schmoll, acting as Agents,  
–        the Romanian Government, by E. Gane and A. Wellman, acting as Agents,  
–        the European Commission, by F. Erlbacher, H. Kranenborg and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 22 September 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 88(1) and (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (‘the GDPR’).  
2        The request was made in the course of proceedings between the Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium (Principal Staff Committee for Teachers at the Ministry of Education and Culture of the Land Hessen, Germany) and the Minister des Hessischen Kultusministeriums (Minister for Education and Culture of the Land Hessen, Germany), concerning the lawfulness of a system for the live streaming of classes by videoconference introduced in schools in the Land Hessen (Germany) without the prior consent of the teachers concerned.  
   
Legal context  
   
European Union law  
   
Directive 95/46/EC  
3        Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) was repealed by the GDPR, with effect from 25 May 2018. Article 3 of that directive, entitled ‘Scope’, was worded as follows:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the [EU Treaty, in the version in force prior to the Treaty of Lisbon,] and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
…’  
   
The GDPR  
4        Recitals 8 to 10, 13, 16, 45 and 155 of the GDPR state:  
‘(8)      Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.  
(9)      The objectives and principles of Directive [95/46] remain sound, but it has not prevented fragmentation in the implementation of data protection across the [European] Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive [95/46].  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive [95/46], Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data (“sensitive data”). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.  
…  
(13)      In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators … to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. …  
…  
(16)      This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.  
…  
(45)      Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. …  
…  
(155)      Member State law or collective agreements, including “works agreements”, may provide for specific rules on the processing of employees’ personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.’  
5        Article 1 of the GDPR, entitled ‘Subject matter and objectives’, provides:  
‘1.      This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.  
2.      This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.  
3.      The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.’  
6        Article 2 of that regulation, entitled ‘Material scope’, provides in paragraphs 1 and 2:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the [EU Treaty];  
(c)      by a natural person in the course of a purely personal or household activity;  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
7        Article 4 of that regulation, entitled ‘Definitions’, provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…’  
8        Article 5 of the GDPR, entitled ‘Principles relating to processing of personal data’, states:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (“purpose limitation”);  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);  
(f)      processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
9        Article 6 of that regulation, entitled ‘Lawfulness of processing’, provides in paragraphs 1 to 3:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:   
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;   
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.  
2.      Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.  
3.      The basis for the processing referred to in points (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.  
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.’  
10      In Chapter IX of the GDPR, entitled ‘Provisions relating to specific processing situations’, Article 88, relating to ‘processing in the context of employment’, provides:  
‘1.      Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer’s or customer’s property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.  
2.      Those rules shall include suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.  
3.      Each Member State shall notify to the [European] Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.’  
   
National law  
11      Paragraph 26(1) of the Bundesdatenschutzgesetz (Federal Law on data protection) of 30 June 2017 (BGBl. 2017 I, p. 2097), provides:  
‘Personal data of employees may be processed for the purposes of an employment relationship where this is necessary for the decision on the establishment of an employment relationship or, after the establishment of the employment relationship, for the implementation or termination of that relationship, and for the exercise or discharge of the rights and obligations arising, respectively, from the representation of employees’ interests and laid down by a law or a collective labour regulation instrument or a works or service agreement (collective agreement). …’  
12      Under Paragraph 23 of the Hessisches Datenschutz- und Informationsfreiheitsgesetz (Law on data protection and freedom of information of the Land Hessen) of 3 May 2018 (‘the HDSIG’):  
‘1.      Personal data of employees may be processed for the purposes of an employment relationship where this is necessary for the decision on the establishment of an employment relationship or, after the establishment of the employment relationship, for the implementation, termination or administration of that relationship, and for the implementation of internal planning, organisational, social and personnel measures. …  
2.      Where the personal data of employees is processed on the basis of consent, account must be taken, in particular, of the dependency of the employee in the employment relationship and the circumstances in which that consent was given when assessing whether the consent was given freely. The free nature of consent may be established, in particular, if there is a legal or economic advantage for the employee, or if the employer and the employee have convergent interests. Consent must be made in writing unless another form is required because of special circumstances. The employer is required to inform the employee in writing of the purpose of the data processing operation and of his or her right to withdraw consent, as provided for in Article 7(3) of the [GDPR].  
3.      By way of derogation from Article 9(1) of [the GDPR], the processing of special categories of personal data within the meaning of Article 9(1) of [the GDPR] shall be permitted for the purposes of the employment relationship where it is necessary for the exercise of rights or for compliance with legal obligations under employment law, or social security and social protection law, and there is no reason to consider that the data subject’s legitimate interest in excluding processing takes precedence. Subparagraph 2 shall also apply to consent to the processing of special categories of personal data. In that regard, the consent must make express reference to those data. …  
4.      The processing of personal data, including special categories of personal data of employees, for the purposes of an employment relationship is permitted on the basis of collective agreements. In so doing, the negotiating parties shall comply with Article 88(2) [of the GDPR].  
5.      The controller must take appropriate measures to ensure that, in particular, the principles for the processing of personal data set out in Article 5 [of the GDPR] are complied with.  
…  
7.      Subparagraphs 1 to 6 shall also apply where personal data, including special categories of personal data, of employees are processed without that data being contained or being intended to be contained in a filing system. The provisions of the Hessisches Beamtengesetz [(HBG) (Law on the civil service of the Land Hessen) of 21 April 2018 (“the HBG”)] applicable to staff cases shall apply   
mutatis mutandis  
 to public sector workers, unless otherwise provided for in the collective labour regulation instrument.  
8.      The following are employees for the purposes of this law:  
1.      workers, including temporary agency workers in the relationship with the user;  
…  
7.      civil servants subject to the [HBG], senior judges of the   
Land  
 and persons performing a civil service.  
…’  
13      Paragraph 86(4) of the HBG provides:  
‘The employer may collect personal data on applicants, civil servants and former civil servants only if this is necessary for the establishment, implementation, termination or administration of the employment relationship or for the implementation of organisational, social and personnel measures, in particular for the purposes of human resources planning and deployment, or if it is permitted by a legal provision or a service agreement. …’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
14      As is apparent from the file submitted to the Court, by two measures adopted in 2020, the Minister for Education and Culture of the Land Hessen established the legal and organisational framework for school education during the COVID-19 pandemic. That framework made it possible, inter alia, for pupils who could not be present in a classroom to attend classes live by videoconference. In order to safeguard pupils’ rights in relation to the protection of personal data, it was established that connection to the videoconference service would be authorised only with the consent of the pupils themselves or, for those pupils who were minors, of their parents. However, no provision was made for the consent of the teachers concerned to their participation in that service.  
15      The Principal Staff Committee for Teachers at the Ministry of Education and Culture of the Land Hessen brought an action before the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), complaining that the live streaming of classes by videoconference was not made conditional on the consent of the teachers concerned.  
16      The Minister for Education and Culture of the Land Hessen, for his part, contended that the processing of personal data inherent in the live streaming of classes by videoconference was covered by the first sentence of Paragraph 23(1) of the HDSIG, so that it could be conducted without the consent of the teachers concerned being sought.  
17      The Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) states in that regard that, in accordance with the intention of the legislature of the Land Hessen, Paragraph 23 of the HDSIG and Paragraph 86 of the HBG fall within the category of ‘more specific rules’ for which Member States may make provision, in accordance with Article 88(1) of the GDPR, to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context. However, that court has doubts as to whether the first sentence of Paragraph 23(1) of the HDSIG and Paragraph 86(4) of the HBG are compatible with the requirements laid down in Article 88(2) of the GDPR.  
18      In the first place, the first sentence of Paragraph 23(1) of the HDSIG and Paragraph 86(4) of the HBG rely on ‘necessity’ as the legal basis for the processing of employees’ data. However, the insertion of the principle of ‘necessity’ into that law does not constitute a rule specifying the requirements contained in Article 88(2) of the GDPR, since the processing of data necessary in the context of an employment relationship is already governed by point (b) of the first subparagraph of Article 6(1) of the GDPR.  
19      In addition, the first sentence of Paragraph 23(1) of the HDSIG applies, beyond the actual contractual relationship, to any processing of employees’ data. It follows from point (f) of the first subparagraph of Article 6(1) of the GDPR that, in the case of personal data processing going beyond processing that is strictly necessary under the employment contract, the fundamental rights and freedoms of the data subject, in the present case the employees and civil servants, must be balanced with the legitimate interest pursued by the controller, in the present case the employer. In so far as the first sentence of Paragraph 23(1) of the HDSIG does not provide for such a balancing exercise, that provision cannot be regarded as a specific sectoral norm after the entry into force of the GDPR.  
20      In the second place, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) considers that the mere reference in Paragraph 23(5) of the HDSIG to the fact that the controller must, inter alia, comply with the principles set out in Article 5 of the GDPR does not meet the requirements of Article 88(2) of that regulation. The latter provision requires suitable and specific legislative provisions to be adopted in order to protect the data subjects’ human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity, and monitoring systems at the work place, and is not merely a rule which must additionally be complied with by those who apply a national provision. Those who apply the provision are not the addressees of Article 88(2) of the GDPR.  
21      In those circumstances, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 88(1) of [the GDPR] to be interpreted as meaning that, in order to be a more specific rule for ensuring the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context within the meaning of Article 88(1) of [the GDPR], a provision must meet the requirements imposed on such rules by Article 88(2) of [the GDPR]?  
(2)      If a national rule clearly does not meet the requirements under Article 88(2) of [the GDPR], can it nevertheless remain applicable?’  
22      By a communication received at the Court Registry on 30 November 2021, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) informed the Court that, as a result of amendments to the national legislation governing the territorial jurisdiction of the administrative courts of the Land Hessen, which was to take effect on 1 December 2021, the dispute in the main proceedings had been transferred to the Verwaltungsgericht Frankfurt am Main (Administrative Court, Frankfurt am Main, Germany). By a communication received at the Court Registry on 21 February 2022, the latter court confirmed that transfer and informed the Court of the new role number assigned to the dispute in the main proceedings.  
   
Admissibility of the request for a preliminary ruling  
23      In its written observations, the German Government submitted that the request for a preliminary ruling was inadmissible in so far as the questions referred for a preliminary ruling were not relevant to the outcome of the dispute in the main proceedings. The Court’s answer would not be useful to the referring court if the processing of the data were authorised by reason of the teacher’s consent. However, the referring court does not explain why it does not take such a possibility into account.  
24      When questioned on this point at the hearing before the Court, the German Government nevertheless acknowledged that the questions referred for a preliminary ruling were relevant where the teacher’s consent could not be obtained.  
25      In that regard, it should be noted that, according to settled case-law, questions referred for a preliminary ruling by a national court in the legislative and factual context which that court is responsible for defining, and the accuracy of which is not a matter for the Court of Justice to determine, enjoy a presumption of relevance. The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 48 and the case-law cited).  
26      In the present case, it is apparent from the order for reference that the parties to the main proceedings disagree as to whether the introduction of live streaming of a class by videoconference systems requires, not only the consent of the parents for their children or that of the pupils who have attained majority, but also the consent of the teachers concerned, or whether, on the other hand, the processing of their personal data is covered by the first sentence of Paragraph 23(1) of the HDSIG and Paragraph 86(4) of the HBG.  
27      It should also be noted that the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) stated in its request for a preliminary ruling, first, that the national legislature considered that Paragraph 23 of the HDSIG and Paragraph 86 of the HBG constitute more specific rules within the meaning of Article 88 of the GDPR and, second, that the outcome of the dispute in the main proceedings depends on whether the first sentence of Paragraph 23(1) of the HDSIG and Paragraph 86(4) of the HBG satisfy the requirements of Article 88 of the GDPR, so as to constitute more specific rules applicable to the processing of the personal data of teachers when classes are livestreamed by the videoconference system at issue in the main proceedings.  
28      In the light of the information thus provided in the request for a preliminary ruling, the arguments put forward by the German Government are not capable of rebutting the presumption of relevance enjoyed by the questions referred.  
29      In those circumstances, the view cannot be taken either that the interpretation of the provisions of EU law that is sought clearly bears no relation to the actual facts of the main action or its purpose, or that the problem is hypothetical, since the referring court is likely to take that interpretation into account for the purposes of resolving the dispute in the main proceedings. Lastly, the Court has before it the factual and legal material necessary to give a useful answer to the questions submitted to it.  
30      Therefore the request for a preliminary ruling is admissible.  
   
Consideration of the questions referred for a preliminary ruling  
   
Preliminary observations  
31      The questions referred for a preliminary ruling concern the interpretation of Article 88(1) and (2) of the GDPR in a dispute relating to the processing of teachers’ personal data during the live streaming by videoconference of the public educational classes which they are responsible for providing.  
32      In the first place, it must be determined whether that processing falls within the material scope of the GDPR, having regard to the fact that, under Article 2(2)(a) of the GDPR, that regulation does not apply to the processing of personal data carried out ‘in the course of an activity which falls outside the scope of Union law’ and that, in accordance with Article 165(1) TFEU, Member States are responsible for the content of teaching and the organisation of their education systems.  
33      In that regard, it is clear from the case-law of the Court that the definition of the material scope of the GDPR, as set out in Article 2(1) of that regulation, is very broad and that the exceptions to that scope, as provided for in Article 2(2) thereof, must be interpreted restrictively (see, to that effect, judgments of 9 July 2020,   
Land   
Hessen  
, C-272/19, EU:C:2020:535, paragraph 68, and of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraphs 61 and 62).   
34      In addition, Article 2(2)(a) of the GDPR is to be read in conjunction with Article 2(2)(b) and recital 16 of that regulation, which states that that regulation does not apply to the processing of personal data in the context of ‘activities which fall outside the scope of Union law, such as activities concerning national security’ and ‘activities in relation to the common foreign and security policy of the Union’ (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 63).  
35      It follows that Article 2(2)(a) and (b) of the GDPR, which partly represents a continuation of the first indent of Article 3(2) of Directive 95/46, cannot be interpreted in broader terms than the exception resulting from the first indent of Article 3(2) of Directive 95/46, a provision which already excluded from that directive’s scope, inter alia, the processing of personal data taking place in the course ‘of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the [EU Treaty, in the version in force prior to the Treaty of Lisbon,] and in any case … processing operations concerning public security, defence, State security’ (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 64).   
36      In the present case, it is common ground that the activity relating to the organisation of teaching in the Land Hessen cannot be classified in the category of activities intended to preserve national security, referred to in Article 2(2)(a) of the GDPR.  
37      Therefore, the processing of teachers’ personal data as part of the live streaming by videoconference of the public educational classes which they provide, such as that at issue in the main proceedings, falls within the material scope of the GDPR.  
38      In the second place, it is apparent from the request for a preliminary ruling that teachers whose personal data processing is at issue in the main proceedings are part of the public service of the Land Hessen, as employees or civil servants.  
39      Therefore, it is necessary to determine whether such processing of personal data falls within the scope of Article 88 of the GDPR, which refers to ‘the processing of employees’ personal data in the employment context’.  
40      In that regard, it should be pointed out that the GDPR does not define the terms ‘employees’ and ‘employment’, nor does it refer to the law of the Member States to define those terms. In the absence of any such reference, it should be recalled that, as follows from the need for a uniform application of EU law and from the principle of equality, the terms of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union (judgment of 2 June 2022,   
HK  
/  
Danmark   
and   
HK  
/  
Privat  
, C-587/20, EU:C:2022:419, paragraph 25 and the case-law cited).  
41      Furthermore, since the GDPR does not define the terms ‘employed’ and ‘employment’, they must be interpreted by reference to their usual meaning in everyday language, while also taking into account the context in which they occur and the purposes of the rules of which they are part (judgment of 2 June 2022,   
HK/   
Danmark   
and   
HK/   
Privat  
, C-587/20, EU:C:2022:419, paragraph 26 and the case-law cited).  
42      The term ‘employee’ in its usual meaning refers to a person who performs his or her work in the context of a relationship of subordination with his or her employer and therefore under the latter’s control (judgment of 18 March 2021,   
Kuoni Travel  
, C-578/19, EU:C:2021:213, paragraph 42).  
43      Likewise, the essential feature of an ‘employment relationship’ is that for a certain period of time a person performs services for and under the direction of another person in return for which he or she receives remuneration (judgment of 15 July 2021,   
Ministrstvo za obrambo  
, C-742/19, EU:C:2021:597, paragraph 49).  
44      Since such a characteristic is specific to employees and to employment both in the public and in the private sector, it must be inferred that the terms ‘employee’ and ‘employment’, understood in their usual sense, do not exclude persons who pursue their professional activity in the public sector.  
45      The scope of Article 88(1) of the GDPR cannot be determined by reference to the nature of the legal relationship that binds the employee to the employer. Thus, it is irrelevant whether the data subject is employed as an employee or as a civil servant, or even whether the terms on which he or she is employed come under public or private law, since those legal designations are varied at the whim of national legislatures and cannot therefore provide an appropriate criterion for a uniform and autonomous interpretation of that provision (see, by analogy, judgments of 12 February 1974,   
Sotgiu  
, 152/73, EU:C:1974:13, paragraph 5, and of 3 June 1986,   
Commission  
 v   
France  
, 307/84, EU:C:1986:222, paragraph 11).  
46      Specifically with regard to persons whose employment relationship is not an employment contract, such as civil servants, it is true that Article 88 of the GDPR refers, in paragraph 1, to the ‘performance of the contract of employment’. However, it should be noted, first, that that reference is among other purposes of the processing of personal data in the employment context which may be the subject of more specific rules adopted by the Member States, listed in Article 88(1) of the GDPR, and that, in any event, that list is not exhaustive, as is demonstrated by the adverbial phrase ‘in particular’ used in that provision.   
47      Second, the irrelevance of the classification of the legal relationship between the employee and the administration employing that employee is borne out by the fact that the management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, the protection of employer’s or customer’s property, the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and the termination of the employment relationship, which are also listed in Article 88(1) of the GDPR, relate to employment in both the private and the public sectors.   
48      Consequently, it cannot be inferred from the reference to the ‘performance of the contract of employment’ in Article 88(1) of the GDPR that employment in the public sector that is not based on an employment contract is excluded from the scope of that provision.   
49      The same conclusion must be reached in relation to the fact that Article 88(2) of the GDPR mentions, among the three factors to which the Member States must have ‘particular regard’ when adopting those ‘more specific rules’, the transfer of personal data ‘within a group of undertakings, or a group of enterprises engaged in a joint economic activity’. The other two factors, namely the transparency of processing and monitoring systems at the work place, are relevant both to employment in the private sector and to employment in the public sector, whatever the nature of the legal relationship that binds the employee to the employer.  
50      The interpretation arising from the wording of Article 88 of the GDPR is confirmed by the context of that article and by the objective pursued by the legislation of which it forms part.   
51      As is apparent from Article 1(1) of the GDPR, read in the light, inter alia, of recitals 9, 10 and 13, that regulation seeks to ensure the harmonisation of national legislation on the protection of personal data which is, in principle, complete. However, the provisions of that regulation make it possible for Member States to lay down additional, stricter or derogating national rules and leave them a margin of discretion as to the manner in which those provisions may be implemented (‘opening clauses’) (see, to that effect, judgment of 28 April 2022,   
Meta Platforms Ireland  
, C-319/20, EU:C:2022:322, paragraph 57).  
52      Article 88 of the GDPR, which forms part of Chapter IX of that regulation entitled ‘Provisions relating to specific processing situations’, constitutes such an opening clause, since it gives Member States the option of adopting ‘more specific rules’ to ensure protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context.  
53      The specific features of the processing of personal data in the employment context and, consequently, the option given to Member States by Article 88(1) of the GDPR are explained, in particular, by the existence of a relationship of subordination between the employee and the employer and not by the nature of the legal relationship that binds the employee to the employer.  
54      Furthermore, under Article 1(2) of the GDPR, read in conjunction with recital 10, that regulation has the objective in particular of ensuring a high level of protection of the fundamental rights and freedoms of natural persons with respect to the processing of personal data; that right is also recognised in Article 8 of the Charter of Fundamental Rights of the European Union and is closely connected to the right to respect for private life, enshrined in Article 7 of that charter (see, to that effect, judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 61).  
55      It is consistent with that objective to apply a broad interpretation of Article 88(1) of the GDPR, according to which the ‘more specific rules’ which the Member States may lay down to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context are likely to apply to all employees, irrespective of the nature of the legal relationship that binds them to their employer.  
56      In those circumstances, the processing of teachers’ personal data during the live streaming, by videoconference, of the public educational classes which they provide, such as that at issue in the main proceedings, falls within the material and personal scope of the GDPR.  
   
The first question  
57      By its first question, the referring court asks, in essence, whether Article 88 of the GDPR must be interpreted as meaning that, in order to be classified as a more specific rule within the meaning of paragraph 1 of that article, a rule of law must satisfy the conditions laid down in paragraph 2 of that article.  
58      As has been pointed out in paragraph 52 above, the Member States have the option, and not the obligation, to adopt such rules, which may be provided for by law or by means of collective agreements.  
59      Furthermore, when the Member States exercise the option granted to them by the opening clause of the GDPR, they must use their discretion under the conditions and within the limits laid down by the provisions of that regulation and must therefore legislate in such a way as not to undermine the content and objectives of that regulation (see, to that effect, judgment of 28 April 2022,   
Meta Platforms Ireland  
, C-319/20, EU:C:2022:322, paragraph 60).  
60      In order to determine the conditions and limits to which the rules referred to in Article 88(1) and (2) of the GDPR are subject and, consequently, to assess the discretion left to the Member States by those provisions, it must be recalled that, in accordance with settled case-law, the interpretation of a provision of EU law requires account to be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 15 March 2022,   
Autorité des marchés financiers  
, C-302/20, EU:C:2022:190, paragraph 63).  
61      As regards the wording of Article 88(1) of the GDPR, it is apparent, first of all, from the use of the words ‘more specific’ that the rules referred to in that provision must have a normative content specific to the area regulated, which is distinct from the general rules of that regulation.  
62      Next, as has been pointed out in paragraph 52 above, the objective of the rules adopted on the basis of that provision is to protect employees’ rights and freedoms in respect of the processing of their personal data in the employment context.  
63      Lastly, it follows from the different purposes for which the processing of personal data may be carried out, as set out in Article 88(1) of the GDPR, that the ‘more specific rules’ to which it refers may relate to a very large number of processing operations in connection with an employment relationship, so as to cover all the purposes for which the processing of personal data may be carried out in the context of an employment relationship. Furthermore, since the listing of those objectives is not exhaustive, as has been pointed out in paragraph 46 above, the Member States have a margin of discretion as regards the processing which is thus subject to those more specific rules.   
64      Article 88 of the GDPR provides, in paragraph 2, that the rules adopted on the basis of paragraph 1 are to include suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights, having particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity, and monitoring systems at the work place.  
65      Thus, it is apparent from the wording of Article 88 of the GDPR that paragraph 2 of that article circumscribes the discretion of those Member States which intend to adopt ‘more specific rules’ under paragraph 1 of that article. Therefore, first, those rules cannot be limited to reiterating the provisions of that regulation and must seek to protect employees’ rights and freedoms in respect of the processing of their personal data in the employment context and include suitable and specific measures to protect the data subjects’ human dignity, legitimate interests and fundamental rights.  
66      Second, particular regard must be had to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity, and monitoring systems at the work place.  
67      As regards the context of Article 88 of the GDPR, it should be noted, in the first place, that that provision must be interpreted in the light of recital 8 of that regulation, according to which, where that regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of that regulation into their national law.  
68      In the second place, it must be borne in mind that Chapters II and III of the GDPR set out, respectively, the principles governing the processing of personal data and the rights of the data subject with which any processing of personal data must comply (judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 50).  
69      In particular, all processing of personal data must comply, first, with the principles relating to processing of data set out in Article 5 of the GDPR and, second, with one of the principles relating to lawfulness of processing listed in Article 6 of that regulation (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 96 and the case-law cited).  
70      As regards the principles relating to the lawfulness of processing, Article 6 of the GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being regarded as legitimate, processing must fall within one of the cases provided for in Article 6 (judgment of 22 June 2021,  
 Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 99 and the case-law cited).  
71      Therefore, although, when exercising the option granted to them by an opening clause of the GDPR, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of that regulation into their national law, the ‘more specific rules’, adopted on the basis of Article 88(1) of that regulation, cannot be limited to a reiteration of the conditions for the lawfulness of personal data processing and the principles of that processing, set out, respectively, in Article 6 and Article 5 of that regulation, or to a reference to those conditions and principles.  
72      The interpretation that the discretion of the Member States, when adopting rules on the basis of Article 88(1) of the GDPR, is limited by paragraph 2 of that article, is consistent with the objective of that regulation, recalled in paragraph 51 above, which is to ensure the harmonisation of national legislation on the protection of personal data which is, in principle, complete.  
73      As the Advocate General observed, in essence, in points 56, 70 and 73 of his Opinion, the possibility for Member States to adopt ‘more specific rules’ on the basis of Article 88(1) of the GDPR may lead to a lack of harmonisation within the scope of those rules. The conditions imposed by Article 88(2) of that regulation reflect the limits of the differentiation accepted by that regulation, in that that lack of harmonisation may be accepted only where the differences that remain are accompanied by specific and suitable safeguards intended to protect employees’ rights and freedoms with regard to the processing of their personal data in the employment context.  
74      Consequently, in order to be classified as a ‘more specific rule’ within the meaning of Article 88(1) of the GDPR, a rule of law must satisfy the conditions laid down in paragraph 2 of that article. Apart from having a normative content specific to the area regulated, which is distinct from the general rules of that regulation, those more specific rules must seek to protect employees’ rights and freedoms in respect of the processing of their personal data in the employment context and include suitable and specific measures to protect the data subjects’ human dignity, legitimate interests and fundamental rights. Particular regard must be had to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity, and monitoring systems at the work place.  
75      In the light of all the foregoing, the answer to the first question is that Article 88 of the GDPR must be interpreted as meaning that national legislation cannot constitute a ‘more specific rule’, within the meaning of paragraph 1 of that article, where it does not satisfy the conditions laid down in paragraph 2 of that article.  
   
The second question  
76      By its second question, the referring court asks, in essence, what conclusions should be drawn from a finding that national provisions adopted to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context are incompatible with the conditions and limits laid down in Article 88(1) and (2) of the GDPR.  
77      In that regard, it must be borne in mind that, under the second paragraph of Article 288 TFEU, a regulation is to be binding in its entirety and is to be directly applicable in all Member States, so that its provisions do not, as a general rule, require the adoption of any implementing measures by the Member States (judgment of 15 June 2021,   
Facebook Ireland and Others  
, C-645/19, EU:C:2021:483, paragraph 109).  
78      However, as has been recalled in paragraph 51 above, opening clauses provided for by the GDPR allow Member States the possibility of laying down additional, stricter or derogating national rules and leave them a margin of discretion as to the way in which the provisions concerned may be implemented.  
79      As has been noted in paragraph 59 above, when the Member States exercise the option granted to them by an opening clause of the GDPR, they must use their discretion under the conditions and within the limits laid down by the provisions of that regulation and must therefore legislate in such a way as not to undermine the content and objectives of that regulation.  
80      It is for the referring court, which alone has jurisdiction to interpret national law, to assess whether the provisions at issue in the main proceedings comply with the conditions and limits laid down in Article 88 of the GDPR, as summarised in paragraph 74 above.  
81      However, as the Advocate General observed in points 60 to 62 of his Opinion, provisions such as Paragraph 23(1) of the HDSIG and Paragraph 86(4) of the HBG, which make the processing of employees’ personal data subject to the condition that such processing is necessary for certain purposes connected with the performance of an employment relationship, appear to reiterate the condition for general lawfulness of processing already set out in point (b) of the first subparagraph of Article 6(1) of the GDPR, without adding a more specific rule within the meaning of Article 88(1) of that regulation. Indeed, such provisions do not appear to have a normative content specific to the area regulated, which is distinct from the general rules of that regulation.  
82      If the referring court were to find that the provisions at issue in the main proceedings do not comply with the conditions and limits laid down in Article 88 of the GDPR, it would, in principle, be required to disregard those provisions.   
83      In accordance with the principle of the primacy of EU law, provisions of the Treaties and directly applicable measures of the institutions have the effect, in their relations with the internal law of the Member States, merely by entering into force, of rendering automatically inapplicable any conflicting provision of national law (judgments of 9 March 1978,   
Simmenthal  
, 106/77, EU:C:1978:49, paragraph 17; of 19 June 1990,   
Factortame and Others  
, C-213/89, EU:C:1990:257, paragraph 18; and of 4 February 2016,   
Ince  
, C-336/14, EU:C:2016:72, paragraph 52).  
84      Therefore, in the absence of more specific rules that comply with the conditions and limits prescribed by Article 88 of the GDPR, the processing of personal data in the employment context, both in the private and public sectors, is directly governed by the provisions of that regulation.  
85      In that regard, it should be noted that points (c) and (e) of the first subparagraph of Article 6(1) of the GDPR, under which the processing of personal data is lawful where that processing is necessary, respectively, for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller, may apply to the processing of personal data such as that at issue in the main proceedings.  
86      Article 6(3) of the GDPR provides, first, with regard to those two situations where processing is lawful, referred to respectively in points (c) and (e) of the first subparagraph of Article 6(1) of that regulation, that the processing must be based on EU law or on Member State law to which the controller is subject and adds, secondly, that the purposes of the processing are to be determined in that legal basis or, as regards the processing referred to in point (e) of the first subparagraph of Article 6(1), are to be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (see, to that effect, judgment of 8 December 2022,   
Inspektor v Inspektorata kam Visshia sadeben savet   
(Purposes of the processing of personal data – Criminal investigation)  
, C-180/21, EU:C:2022:967, paragraph 95).  
87      It should be pointed out that the Court has already held that lawful processing of personal data by the controllers on the basis of point (e) of the first subparagraph of Article 6(1) of the GDPR presupposes not only that they can be regarded as performing a task carried out in the public interest, but also that the processing of personal data for the purpose of performing such a task is founded on a legal basis referred to in Article 6(3) of that regulation (see, to that effect, judgment of 20 October 2022,   
Koalitsia ‘Demokratichna Bulgaria – Obedinenie’  
, C-306/21, EU:C:2022:813, paragraph 52).  
88      Consequently, where the referring court finds that the national provisions on the processing of personal data in the employment context do not comply with the conditions and limits laid down in Article 88(1) and (2) of the GDPR, it must still verify whether those provisions constitute a legal basis referred to in Article 6(3) of that regulation, read in conjunction with recital 45, which complies with the requirements laid down in that regulation. If that is the case, the national provisions must not be disregarded.  
89      In the light of the foregoing, the answer to the second question referred for a preliminary ruling is that Article 88(1) and (2) of the GDPR must be interpreted as meaning that the application of national provisions adopted to ensure the protection of employees’ rights and freedoms in respect of the processing of their personal data in the employment context must be disregarded where those provisions do not comply with the conditions and limits laid down in Article 88(1) and (2), unless those provisions constitute a legal basis referred to in Article 6(3) of that regulation, which complies with the requirements laid down by that regulation.  
   
Costs  
90      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
1.        
Article 88 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
must be interpreted as meaning that national legislation cannot constitute a ‘more specific rule’, within the meaning of paragraph 1 of that article, where it does not satisfy the conditions laid down in paragraph 2 of that article.  
2.        
Article 88(1) and (2) of Regulation 2016/679  
must be interpreted as meaning that the application of national provisions adopted to ensure the protection of employees’ rights and freedoms in respect of the processing of their personal data in the employment context must be disregarded where those provisions do not comply with the conditions and limits laid down in Article 88(1) and (2), unless those provisions constitute a legal basis referred to in Article 6(3) of that regulation, which complies with the requirements laid down by that regulation.

ID: 9fb268dd-1da3-4b55-acf1-42ab547cfc73

Judgment of 12 Dec 2013, C-486/12 (  
X  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
   
JUDGMENT OF THE COURT (Eighth Chamber)  
12 December 2013 (\*)  
(Protection of individuals with regard to the processing of personal data – Directive 95/46/EC – Conditions for exercising a right of access – Levying of excessive fees)  
In Case C-486/12,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Gerechtshof te ’s-Hertogenbosch (Netherlands), made by decision of 26 October 2012, received at the Court on 31 October 2012, in the proceedings brought by  
X  
THE COURT (Eighth Chamber),  
composed of C.G. Fernlund (Rapporteur), President of the Chamber, C. Toader and E. Jarašiūnas, Judges,  
Advocate General: Y. Bot,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        the Netherlands Government, by B. Koopman and C. Wissels, acting as Agents,  
–        the Czech Government, by M. Smolek, acting as Agent,  
–        the Hungarian Government, by M.Z. Fehér and by K. Szíjjártó and K. Molnár, acting as Agents,  
–        the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,  
–        the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,  
–        the United Kingdom Government, by J. Beeko, acting as Agent, assisted by J. Holmes, Barrister,  
–        the European Commission, by B. Martenczuk and P. van Nuffel, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 12 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings brought by X concerning payment of a fee for delivery of a certified transcript containing personal data.  
   
Legal context  
   
European Union (‘EU’) law  
3        Article 12 of Directive 95/46, entitled ‘Right of access’, provides:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
(a)      without constraint at reasonable intervals and without excessive delay or expense:  
–        confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,  
–        communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,  
–        knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
(c)      notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.’  
   
Netherlands law  
4        Article 79 of the Wet gemeentelijke basisadministratie persoonsgegevens (Law on personal data held by local authorities) (Stb. 1994 No 494) (‘the Wet GBA’) provides:  
‘1.      The College shall inform anyone, on request, in writing, within four weeks and free of charge, whether personal data relating to that person are being processed in the database. In so far as such data are being processed, the person making the request regarding the municipal database must receive the written notification referred to in Article 78(3). …   
2.      The College shall provide anyone, on request, within four weeks and free of charge, with access to the data relating to that person contained in the database. …  
3.      The College shall provide anyone, on request, within four weeks, with a transcript (certified if required), in an intelligible form, of the personal data relating to him which are being processed in the database, and the available information on the source of such data in so far as the person making the request is not himself the source. …’  
5        Article 229 of the Gemeentewet (Law on municipalities) is worded as follows:  
‘1.      Duties may be levied on:  
…  
(b)      the use of services provided by or on behalf of the municipal authorities;  
…’  
6        Article 229b(1) of the Gemeentewet provides:  
‘In the Regulations on the basis of which duties as referred to in Article 229(1)(a) and (b) are levied, the rates shall be set in such a way that the estimated income from the duties does not exceed the estimated expenditure related thereto. …’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
7        In proceedings contesting a decision imposing a fine on X for a traffic offence, X sought to show that she had never received the notices requesting payment of that fine, as they had been sent to the wrong address. To that end, X asked her municipality of residence to disclose her personal data for the years 2008 and 2009, in particular her various addresses. In response, the municipality provided a certified transcript of the personal data in question pursuant to Article 79(3) of the Wet GBA and, in exchange, demanded payment of a fee of EUR 12.80.  
8        X brought an action contesting that request for payment, but was unsuccessful. In her appeal before the Gerechtshof te ’s-Hertogenbosch (Regional Court of Appeal, te ’s-Hertogenbosch; or ‘the referring court’), X claims not to have requested a certified transcript, but simply to have sought to obtain her personal data on the basis of the Wet Openbaarheid van Bestuur (Law on open government). In the light of that legal basis, X argues that no fees should have been levied.  
9        For its part, the municipality contends that the personal data in question cannot be provided in any way other than by certified transcript pursuant to Article 79(3) of the Wet GBA. As provision of a transcript to an individual is connected with satisfying the private interests of that individual, it is a service in respect of which, under Article 229(1)(b) of the Gemeentewet, payment of a fee may be required.  
10      The referring court observes that (i) certified transcripts of personal data are the only ones to be officially recognised and used by the public authorities and (ii) the provision of data from municipal files falls within the scope of Directive 95/46, regardless of the basis, in national law, for the request for access to such data.  
11      According to that court, Article 12(a) of Directive 95/46 guarantees every data subject the right to obtain, without constraint, at reasonable intervals and without excessive delay or expense, communication to him in an intelligible form of the personal data undergoing processing and of any available information as to their source. That court is also of the view that Article 12(a) of Directive 95/46 can be construed in two ways:  
–        the communication of personal data must take place without excessive delay or excessive expense, or  
–        the communication of personal data must take place without excessive delay and without expense.  
12      In the former case, it is permissible to levy a fee, so long as it is not excessive. In the latter case, levying a fee is prohibited.  
13      As regards the issue of whether the fee in question is excessive, the referring court observes that, under Article 229b of the Gemeentewet, the rates are to be set in such a way that the income from that fee does not exceed the related expenditure. However, that is no guarantee that the income from fees will not be higher than the expenditure related to the communication of personal data. The referring court is also uncertain as to the exact point at which fees levied may be regarded as excessive for the purposes of Article 12(a) of Directive 95/46.  
14      If it is found that Article 12(a) of Directive 95/46 must be interpreted as meaning that personal data is to be communicated free of charge, the referring court is uncertain as to whether it is necessary to provide an alternative to the provision of a transcript which must be paid for pursuant to Article 79(3) of the Wet GBA, perhaps by allowing data to be viewed on a display screen. However, it points out that access to a display screen does not constitute a communication for the purposes of Article 12(a) of the directive and that Article 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’) protects only the right to access data. Access to data via a display screen has the additional disadvantage that, unlike a certified transcript, it cannot be accepted as authentic and accurate by the public authorities (Case C-553/07   
Rijkeboer  
 [2009] ECR I-3889) and cannot provide a historical overview of the data registered.  
15      In those circumstances, the Gerechtshof te’s-Hertogenbosch decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘1.      Does the provision of access [to data] (pursuant to Article 79(2) of the Wet GBA) constitute compliance with the obligation [to communicate] data undergoing processing as referred to in the second indent of Article 12(a) of Directive [95/46/EC]?  
2.      Does Article 12(a) of [that directive] preclude the levying of fees in respect of the communication, by means of a transcript from the municipal database, of the personal data undergoing processing?  
3.      If Question 2 is to be answered in the negative: is the levying of the present fee excessive [for the purposes of] Article 12(a) of [that directive]?’  
   
Consideration of the questions referred  
   
Question 2  
16      By its second question, which it is appropriate to examine first, the referring court asks, in essence, whether Article 12(a) of Directive 95/46 is to be interpreted as precluding the levying of fees in respect of the communication of personal data by a public authority.  
17      All the Member States which have submitted written observations to the Court maintain, as does the European Commission, that Article 12(a) of Directive 95/46 allows public authorities to require payment of fees in respect of the communication of personal data referred to in that provision, so long as those fees are not excessive.  
18      It should be pointed out that the Dutch-language version of Article 12(a) of Directive 95/46 uses the phrase ‘bovenmatige vertraging of kosten’. That wording might be thought to suggest that the adjective ‘bovenmatige’ (‘excessive’) relates only to delays (‘vertraging’), thereby suggesting that the right to obtain communication of the data referred to in that provision should not be subject to the payment of fees.  
19      However, for the purposes of its interpretation, Article 12(a) of Directive 95/46 cannot be examined solely in the Dutch-language version: according to settled case-law, the need for the uniform application of an EU measure and, accordingly, for a uniform interpretation of that measure makes it impossible to consider one version of the text in isolation, but requires that it be interpreted on the basis of both the real intention of its author and the aim which the latter seeks to achieve, in the light, in particular, of the versions in all languages (see, inter alia, Case 29/69   
Stauder  
 [1969] ECR I-419, paragraph 3; Case C-280/04   
Jyske Finans  
 [2005] ECR I-10683, paragraph 31; and Case C-445/09   
IMC Securities  
 [2011] ECR I-5917, paragraph 25).  
20      There is nothing in the non-Dutch-language versions of Article 12(a) of Directive 95/46 to suggest that Member States are required to communicate the information referred to in that provision free of charge. On the contrary, other versions of that provision – for example, the Spanish (‘sin retrasos ni gastos excesivos’), Danish (‘uden større ventetid eller større udgifter’), German (‘ohne unzumutbare Verzögerung oder übermäβiger Kosten’), French (‘sans délais ou frais excessifs’), Italian (‘senza ritardi o spese eccessivi’), Portuguese (‘sem demora ou custos excessivos’) and Finnish (‘aiheetonta viivyvtystä tai aiheettomia kustannuksia’) – indicate that Member States are merely required to communicate such information without levying excessive fees.  
21      It is true that some language versions of the provision in question – such as the English (‘without excessive delay or expense’) and Swedish (‘större tidsutdräkt eller kostnader’) versions – are, like the Dutch version, ambiguous in so far as the adjective ‘excessive’ does not explicitly qualify the word ‘expense’. However, none of the language versions of that provision unequivocally states that communication must take place free of charge.  
22      It is therefore clear from the wording of Article 12(a) of Directive 95/46 that that provision does not require the Member States to levy fees when the right to access personal data is exercised; nor, however, does it prohibit the levying of such fees, so long as they are not excessive.  
23      Consequently, the answer to Question 2 is that Article 12(a) of Directive 95/46 must be interpreted as not precluding the levying of fees in respect of the communication of personal data by a public authority.  
   
Question 3  
24      By its third question, the referring court seeks to ascertain, in essence, the criteria on the basis of which it is possible to ensure that a fee which is levied when the right to access personal data is exercised is not excessive for the purposes of Article 12(a) of Directive 95/46.  
25      Under that provision, the Member States are to confer upon any person a right of access to personal data relating to him and to information on the recipients or categories of recipients of such data and the logic involved in any automatic processing of such data. In view of the considerations made above in the analysis of Question 2, Article 12(a) of Directive 95/46 must be interpreted as requiring Member States to ensure that the exercise of that right of access takes place without constraint, without excessive delay, and without excessive expense.  
26      Accordingly, it is for the Member States to determine whether communication of the information referred to in Article 12(a) of Directive 95/46 entails the payment of fees and, if so, to set such fees at a level which is not excessive.  
27      However, that provision does not list any criteria for assessing whether fees levied by a Member State when the right of access provided for thereunder is exercised are to be regarded as excessive. In order to establish such criteria, Article 12(a) of Directive 95/46 must be construed with regard to its purpose when examined in the light of the objectives of that directive.  
28      Thus, it is for any Member State which requires payment of a fee from individuals exercising the right to access the data referred to in Article 12(a) of Directive 95/46 to fix that fee at a level which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular through his right to have the data communicated to him in an intelligible form, so that he is able, if necessary, to exercise his rights to rectification, erasure and blocking of the data (in the event that the processing of the data does not comply with the directive) and his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to communicate such data represents for the controller (see, by analogy,   
Rijkeboer  
, paragraph 64).  
29      In view of the importance – highlighted in recitals 2 and 10 in the preamble to Directive 95/46 – of protecting privacy, emphasised in the case-law of the Court (see   
Rijkeboer  
, paragraph 47 and the case-law cited) and enshrined in Article 8 of the Charter, the fees which may be levied under Article 12(a) of the directive may not be fixed at a level likely to constitute an obstacle to the exercise of the right of access guaranteed by that provision.  
30      It should be held that, for the purposes of applying Article 12(a) of Directive 95/46, where a national public authority levies a fee on an individual exercising the right to access personal data relating to him, the level of that fee should not exceed the cost of communicating such data. That upper limit does not prevent the Member States from fixing such fees at a lower level in order to ensure that all individuals retain an effective right to access such data.  
31      Accordingly, the answer to Question 3 is that Article 12(a) of Directive 95/46 must be interpreted as meaning that, in order to ensure that fees levied when the right to access personal data is exercised are not excessive for the purposes of that provision, the level of those fees must not exceed the cost of communicating such data. It is for the national court to carry out any verifications necessary, having regard to the circumstances of the case.  
   
Question 1  
32      Question 1 must be understood to arise solely in the event that Article 12(a) of Directive 95/46 is interpreted as precluding the levying of fees in respect of the communication of personal data by a public authority. As it is, in view of the answer to Question 2, there is no need to answer Question 1.  
   
Costs  
33      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Eighth Chamber) hereby rules:  
1.        
Article 12(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as not precluding the levying of fees in respect of the communication of personal data by a public authority.  
2.        
Article 12(a) of Directive 95/46 must be interpreted as meaning that, in order to ensure that fees levied when the right to access personal data is exercised are not excessive for the purposes of that provision, the level of those fees must not exceed the cost of communicating such data. It is for the national court to carry out any verifications necessary, having regard to the circumstances of the case.

ID: a35bf67a-9180-48c4-b5b1-6d7bc4e819d8

Judgment of 13 May 2014, C-131/12 (  
Google Spain and Google  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Processing   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Territorial Scope   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Main Establishment   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to object   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Powers   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to object   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accuracy   
General data protection law   
 >   
Chapter II - Principles   
 >   
Storage limitation   
   
JUDGMENT OF THE COURT (Grand Chamber)  
13 May 2014 (\*)  
(Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator’s obligations and of the data subject’s rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8)  
In Case C-131/12,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012, in the proceedings  
Google Spain SL,  
Google Inc.  
v  
Agencia Española de Protección de Datos (AEPD),  
Mario Costeja González,  
THE COURT (Grand Chamber),  
composed of V. Skouris, President, K. Lenaerts, Vice-President, M. Ilešič (Rapporteur), L. Bay Larsen, T. von Danwitz, M. Safjan, Presidents of Chambers, J. Malenovský, E. Levits, A. Ó Caoimh, A. Arabadjiev, M. Berger, A. Prechal and E. Jarašiūnas Judges,  
Advocate General: N. Jääskinen,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 26 February 2013,  
after considering the observations submitted on behalf of:  
–        Google Spain SL and Google Inc., by F. González Díaz, J. Baño Fos and B. Holles, abogados,   
–        Mr Costeja González, by J. Muñoz Rodríguez, abogado,  
–        the Spanish Government, by A. Rubio González, acting as Agent,  
–        the Greek Government, by E.-M. Mamouna and K. Boskovits, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,  
–        the Austrian Government, by G. Kunnert and C. Pesendorfer, acting as Agents,  
–        the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,  
–        the European Commission, by I. Martínez del Peral and B. Martenczuk, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 25 June 2013,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2(b) and (d), Article 4(1)(a) and (c), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) and of Article 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between, on the one hand, Google Spain SL (‘Google Spain’) and Google Inc. and, on the other, the Agencia Española de Protección de Datos (Spanish Data Protection Agency; ‘the AEPD’) and Mr Costeja González concerning a decision by the AEPD upholding the complaint lodged by Mr Costeja González against those two companies and ordering Google Inc. to adopt the measures necessary to withdraw personal data relating to Mr Costeja González from its index and to prevent access to the data in the future.  
   
Legal context  
   
European Union law  
3        Directive 95/46 which, according to Article 1, has the object of protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and of removing obstacles to the free flow of such data, states in recitals 2, 10, 18 to 20 and 25 in its preamble:  
‘(2)      … data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;  
...  
(10)      … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [, signed in Rome on 4 November 1950,] and in the general principles of Community law; … for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;  
...  
(18)      … in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; … in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;   
(19)      … establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; … the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor in this respect; … when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;  
(20)      … the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; … in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;  
...  
(25)      … the principles of protection must be reflected, on the one hand, in the obligations imposed on persons … responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances’.  
4        Article 2 of Directive 95/46 states that ‘[f]or the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)       “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
...  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;  
...’  
5        Article 3 of Directive 95/46, entitled ‘Scope’, states in paragraph 1:  
‘This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.’  
6        Article 4 of Directive 95/46, entitled ‘National law applicable’, provides:   
‘1.      Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:  
(a)      the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;  
(b)      the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;        
(c)      the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.  
2.      In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.’  
7        In Section I (entitled ‘Principles relating to data quality’) of Chapter II of Directive 95/46, Article 6 is worded as follows:  
‘1.      Member States shall provide that personal data must be:  
(a)      processed fairly and lawfully;  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.  
2.      It shall be for the controller to ensure that paragraph 1 is complied with.’  
8        In Section II (entitled ‘Criteria for making data processing legitimate’) of Chapter II of Directive 95/46, Article 7 provides:  
‘Member States shall provide that personal data may be processed only if:  
...  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
9        Article 9 of Directive 95/46, entitled ‘Processing of personal data and freedom of expression’, provides:  
‘Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.’  
10      Article 12 of Directive 95/46, entitled ‘Rights of access’, provides:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
...  
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
...’  
11      Article 14 of Directive 95/46, entitled ‘The data subject’s right to object’, provides:  
‘Member States shall grant the data subject the right:  
(a)      at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;  
...’  
12      Article 28 of Directive 95/46, entitled ‘Supervisory authority’, is worded as follows:  
‘1.      Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.  
...  
3.      Each authority shall in particular be endowed with:  
–        investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,  
–        effective powers of intervention, such as, for example, that … of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing …   
–        ...  
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.  
4.      Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.  
...  
6.      Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.  
The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.  
...’  
   
Spanish law  
13      Directive 95/46 was transposed into Spanish Law by Organic Law No 15/1999 of 13 December 1999 on the protection of personal data (BOE No 298 of 14 December 1999, p. 43088).  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
14      On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) (‘La Vanguardia’), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr Costeja González’s name in the search engine of the Google group (‘Google Search’), he would obtain links to two pages of La Vanguardia’s newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González’s name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.  
15      By that complaint, Mr Costeja González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. Mr Costeja González stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.  
16      By decision of 30 July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.  
17      On the other hand, the complaint was upheld in so far as it was directed against Google Spain and Google Inc. The AEPD considered in this regard that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where they appear, including when retention of the information on that site is justified by a statutory provision.  
18      Google Spain and Google Inc. brought separate actions against that decision before the Audiencia Nacional (National High Court). The Audiencia Nacional joined the actions.  
19      That court states in the order for reference that the actions raise the question of what obligations are owed by operators of search engines to protect personal data of persons concerned who do not wish that certain information, which is published on third parties’ websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to internet users indefinitely. The answer to that question depends on the way in which Directive 95/46 must be interpreted in the context of these technologies, which appeared after the directive’s publication.  
20      In those circumstances, the Audiencia Nacional decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘1.      With regard to the territorial application of Directive [95/46] and, consequently, of the Spanish data protection legislation:  
(a)      must it be considered that an “establishment”, within the meaning of Article 4(1)(a) of Directive 95/46, exists when any one or more of the following circumstances arise:  
–        when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State,  
or  
–        when the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking,  
or  
–        when the office or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily?  
(b)      Must Article 4(1)(c) of Directive 95/46 be interpreted as meaning that there is “use of equipment … situated on the territory of the said Member State”:  
–        when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State,  
or  
–        when it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State?  
(c)      Is it possible to regard as a use of equipment, in the terms of Article 4(1)(c) of Directive 95/46, the temporary storage of the information indexed by internet search engines? If the answer to that question is affirmative, can it be considered that that connecting factor is present when the undertaking refuses to disclose the place where it stores those indexes, invoking reasons of competition?  
(d)      Regardless of the answers to the foregoing questions and particularly in the event that the Court … considers that the connecting factors referred to in Article 4 of [Directive 95/46] are not present:  
must Directive 95/46 … be applied, in the light of Article 8 of the [Charter], in the Member State where the centre of gravity of the conflict is located and more effective protection of the rights of … Union citizens is possible?  
2.      As regards the activity of search engines as providers of content in relation to Directive 95/46 …:  
(a)      in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of “processing of … data” used in Article 2(b) of Directive 95/46?  
(b)      If the answer to the foregoing question is affirmative, and once again in relation to an activity like the one described:  
must Article 2(d) of Directive 95/46 be interpreted as meaning that the undertaking managing [Google Search] is to be regarded as the “controller” of the personal data contained in the web pages that it indexes?  
(c)      In the event that the answer to the foregoing question is affirmative:  
may the [AEPD], protecting the rights embodied in [Article] 12(b) and [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, directly impose on [Google Search] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located?  
(d)      In the event that the answer to the foregoing question is affirmative:  
would the obligation of search engines to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?  
3.      Regarding the scope of the right of erasure and/or the right to object, in relation to the “derecho al olvido” (the “right to be forgotten”), the following question is asked:  
must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties’ web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?’  
   
Consideration of the questions referred  
   
Question 2(a) and (b), concerning the material scope of Directive 95/46  
21      By Question 2(a) and (b), which it is appropriate to examine first, the referring court asks, in essence, whether Article 2(b) of Directive 95/46 is to be interpreted as meaning that the activity of a search engine as a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of that provision when that information contains personal data. If the answer is in the affirmative, the referring court seeks to ascertain furthermore whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the ‘controller’ in respect of that processing of the personal data, within the meaning of that provision.  
22      According to Google Spain and Google Inc., the activity of search engines cannot be regarded as processing of the data which appear on third parties’ web pages displayed in the list of search results, given that search engines process all the information available on the internet without effecting a selection between personal data and other information. Furthermore, even if that activity must be classified as ‘data processing’, the operator of a search engine cannot be regarded as a ‘controller’ in respect of that processing since it has no knowledge of those data and does not exercise control over the data.  
23      On the other hand, Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the European Commission consider that that activity quite clearly involves ‘data processing’ within the meaning of Directive 95/46, which is distinct from the data processing by the publishers of websites and pursues different objectives from such processing. The operator of a search engine is the ‘controller’ in respect of the data processing carried out by it since it is the operator that determines the purposes and means of that processing.  
24      In the Greek Government’s submission, the activity in question constitutes such ‘processing’, but inasmuch as search engines serve merely as intermediaries, the undertakings which operate them cannot be regarded as ‘controllers’, except where they store data in an ‘intermediate memory’ or ‘cache memory’ for a period which exceeds that which is technically necessary.  
25      Article 2(b) of Directive 95/46 defines ‘processing of personal data’ as ‘any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction’.  
26      As regards in particular the internet, the Court has already had occasion to state that the operation of loading personal data on an internet page must be considered to be such ‘processing’ within the meaning of Article 2(b) of Directive 95/46 (see Case C-101/01   
Lindqvist   
EU:C:2003:596, paragraph 25).  
27      So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus ‘personal data’ within the meaning of Article 2(a) of that directive.  
28      Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine ‘collects’ such data which it subsequently ‘retrieves’, ‘records’ and ‘organises’ within the framework of its indexing programmes, ‘stores’ on its servers and, as the case may be, ‘discloses’ and ‘makes available’ to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as ‘processing’ within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.  
29      Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine.  
30      The Court has already held that the operations referred to in Article 2(b) of Directive 95/46 must also be classified as such processing where they exclusively concern material that has already been published in unaltered form in the media. It has indeed observed in that regard that a general derogation from the application of Directive 95/46 in such a case would largely deprive the directive of its effect (see, to this effect, Case C-73/07   
Satakunnan Markkinapörssi and Satamedia  
 EU:C:2008:727, paragraphs 48 and 49).  
31      Furthermore, it follows from the definition contained in Article 2(b) of Directive 95/46 that, whilst the alteration of personal data indeed constitutes processing within the meaning of the directive, the other operations which are mentioned there do not, on the other hand, in any way require that the personal data be altered.   
32      As to the question whether the operator of a search engine must be regarded as the ‘controller’ in respect of the processing of personal data that is carried out by that engine in the context of an activity such as that at issue in the main proceedings, it should be recalled that Article 2(d) of Directive 95/46 defines ‘controller’ as ‘the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data’.   
33      It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the ‘controller’ in respect of that processing pursuant to Article 2(d).  
34      Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of ‘controller’, effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.  
35      In this connection, it should be pointed out that the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page.  
36      Moreover, it is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject’s name, including to internet users who otherwise would not have found the web page on which those data are published.  
37      Also, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users’ access to that information may, when users carry out their search on the basis of an individual’s name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject.  
38      Inasmuch as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.  
39      Finally, the fact that publishers of websites have the option of indicating to operators of search engines, by means in particular of exclusion protocols such as ‘robot.txt’ or codes such as ‘noindex’ or ‘noarchive’, that they wish specific information published on their site to be wholly or partially excluded from the search engines’ automatic indexes does not mean that, if publishers of websites do not so indicate, the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine’s activity.  
40      That fact does not alter the position that the purposes and means of that processing are determined by the operator of the search engine. Furthermore, even if that option for publishers of websites were to mean that they determine the means of that processing jointly with that operator, this finding would not remove any of the latter’s responsibility as Article 2(d) of Directive 95/46 expressly provides that that determination may be made ‘alone or jointly with others’.   
41      It follows from all the foregoing considerations that the answer to Question 2(a) and (b) is that Article 2(b) and (d) of Directive 95/46 are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the ‘controller’ in respect of that processing, within the meaning of Article 2(d).  
   
Question 1(a) to (d), concerning the territorial scope of Directive 95/46  
42      By Question 1(a) to (d), the referring court seeks to establish whether it is possible to apply the national legislation transposing Directive 95/46 in circumstances such as those at issue in the main proceedings.   
43      In this respect, the referring court has established the following facts:  
–        Google Search is offered worldwide through the website ‘www.google.com’. In numerous States, a local version adapted to the national language exists. The version of Google Search in Spanish is offered through the website ‘www.google.es’, which has been registered since 16 September 2003. Google Search is one of the most used search engines in Spain.  
–        Google Search is operated by Google Inc., which is the parent company of the Google Group and has its seat in the United States.  
–        Google Search indexes websites throughout the world, including websites located in Spain. The information indexed by its ‘web crawlers’ or robots, that is to say, computer programmes used to locate and sweep up the content of web pages methodically and automatically, is stored temporarily on servers whose State of location is unknown, that being kept secret for reasons of competition.  
–        Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users’ search terms, for undertakings which wish to use that tool in order to offer their goods or services to the internet users.  
–        The Google group has recourse to its subsidiary Google Spain for promoting the sale of advertising space generated on the website ‘www.google.com’. Google Spain, which was established on 3 September 2003 and possesses separate legal personality, has its seat in Madrid (Spain). Its activities are targeted essentially at undertakings based in Spain, acting as a commercial agent for the Google group in that Member State. Its objects are to promote, facilitate and effect the sale of on-line advertising products and services to third parties and the marketing of that advertising.  
–        Google Inc. designated Google Spain as the controller, in Spain, in respect of two filing systems registered by Google Inc. with the AEPD; those filing systems were intended to contain the personal data of the customers who had concluded contracts for advertising services with Google Inc.  
44      Specifically, the main issues raised by the referring court concern the notion of ‘establishment’, within the meaning of Article 4(1)(a) of Directive 95/46, and of ‘use of equipment situated on the territory of the said Member State’, within the meaning of Article 4(1)(c).  
 Question 1(a)  
45      By Question 1(a), the referring court asks, in essence, whether Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when one or more of the following three conditions are met:   
–        the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State, or  
–        the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking, or  
–        the branch or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to protection of personal data, even where such collaboration is engaged in voluntarily.  
46      So far as concerns the first of those three conditions, the referring court states that Google Search is operated and managed by Google Inc. and that it has not been established that Google Spain carries out in Spain an activity directly linked to the indexing or storage of information or data contained on third parties’ websites. Nevertheless, according to the referring court, the promotion and sale of advertising space, which Google Spain attends to in respect of Spain, constitutes the bulk of the Google group’s commercial activity and may be regarded as closely linked to Google Search.  
47      Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the Commission submit that, in the light of the inextricable link between the activity of the search engine operated by Google Inc. and the activity of Google Spain, the latter must be regarded as an establishment of the former and the processing of personal data is carried out in context of the activities of that establishment. On the other hand, according to Google Spain, Google Inc. and the Greek Government, Article 4(1)(a) of Directive 95/46 is not applicable in the case of the first of the three conditions listed by the referring court.   
48      In this regard, it is to be noted first of all that recital 19 in the preamble to Directive 95/46 states that ‘establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements’ and that ‘the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor’.  
49      It is not disputed that Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain. As it moreover has separate legal personality, it constitutes a subsidiary of Google Inc. on Spanish territory and, therefore, an ‘establishment’ within the meaning of Article 4(1)(a) of Directive 95/46.  
50      In order to satisfy the criterion laid down in that provision, it is also necessary that the processing of personal data by the controller be ‘carried out in the context of the activities’ of an establishment of the controller on the territory of a Member State.  
51      Google Spain and Google Inc. dispute that this is the case since the processing of personal data at issue in the main proceedings is carried out exclusively by Google Inc., which operates Google Search without any intervention on the part of Google Spain; the latter’s activity is limited to providing support to the Google group’s advertising activity which is separate from its search engine service.  
52      Nevertheless, as the Spanish Government and the Commission in particular have pointed out, Article 4(1)(a) of Directive 95/46 does not require the processing of personal data in question to be carried out ‘by’ the establishment concerned itself, but only that it be carried out ‘in the context of the activities’ of the establishment.  
53      Furthermore, in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively (see, by analogy, Case C-324/09   
L'Oréal and Others  
 EU:C:2011:474, paragraphs 62 and 63).  
54      It is to be noted in this context that it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope.  
55      In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out ‘in the context of the activities’ of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.  
56      In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.  
57      As has been stated in paragraphs 26 to 28 of the present judgment, the very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller’s establishment on the territory of a Member State, in this instance Spanish territory.  
58      That being so, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive’s effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure (see, by analogy,   
L'Oréal and Others  
 EU:C:2011:474, paragraphs 62 and 63), in particular their right to privacy, with respect to the processing of personal data, a right to which the directive accords special importance as is confirmed in particular by Article 1(1) thereof and recitals 2 and 10 in its preamble (see, to this effect, Joined Cases C-465/00, C-138/01 and C-139/01   
 Österreichischer Rundfunk and Others  
 EU:C:2003:294, paragraph 70; Case C-553/07   
Rijkeboer   
EU:C:2009:293, paragraph 47; and Case C-473/12   
IPI   
EU:C:2013:715, paragraph 28 and the case-law cited).  
59      Since the first of the three conditions listed by the referring court suffices by itself for it to be concluded that an establishment such as Google Spain satisfies the criterion laid down in Article 4(1)(a) of Directive 95/46, it is unnecessary to examine the other two conditions.  
60      It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.  
 Question 1(b) to (d)  
61      In view of the answer given to Question 1(a), there is no need to answer Question 1(b) to (d).  
   
Question 2(c) and (d), concerning the extent of the responsibility of the operator of a search engine under Directive 95/46   
62      By Question 2(c) and (d), the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.  
63      Google Spain and Google Inc. submit that, by virtue of the principle of proportionality, any request seeking the removal of information must be addressed to the publisher of the website concerned because it is he who takes the responsibility for making the information public, who is in a position to appraise the lawfulness of that publication and who has available to him the most effective and least restrictive means of making the information inaccessible. Furthermore, to require the operator of a search engine to withdraw information published on the internet from its indexes would take insufficient account of the fundamental rights of publishers of websites, of other internet users and of that operator itself.  
64      According to the Austrian Government, a national supervisory authority may order such an operator to erase information published by third parties from its filing systems only if the data in question have been found previously to be unlawful or incorrect or if the data subject has made a successful objection to the publisher of the website on which that information was published.  
65      Mr Costeja González, the Spanish, Italian and Polish Governments and the Commission submit that the national authority may directly order the operator of a search engine to withdraw from its indexes and intermediate memory information containing personal data that has been published by third parties, without having to approach beforehand or simultaneously the publisher of the web page on which that information appears. Furthermore, according to Mr Costeja González, the Spanish and Italian Governments and the Commission, the fact that the information has been published lawfully and that it still appears on the original web page has no effect on the obligations of that operator under Directive 95/46. On the other hand, according to the Polish Government that fact is such as to release the operator from its obligations.  
66      First of all, it should be remembered that, as is apparent from Article 1 and recital 10 in the preamble, Directive 95/46 seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (see, to this effect,   
IPI   
EU:C:2013:715, paragraph 28).  
67      According to recital 25 in the preamble to Directive 95/46, the principles of protection laid down by the directive are reflected, on the one hand, in the obligations imposed on persons responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals whose data are the subject of processing to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.  
68      The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter (see, in particular, Case C-274/99 P   
Connolly  
 v   
Commission   
EU:C:2001:127, paragraph 37, and  
 Österreichischer Rundfunk and Others  
 EU:C:2003:294, paragraph 68).  
69      Article 7 of the Charter guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data. Article 8(2) and (3) specify that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that everyone has the right of access to data which have been collected concerning him or her and the right to have the data rectified, and that compliance with these rules is to be subject to control by an independent authority. Those requirements are implemented inter alia by Articles 6, 7, 12, 14 and 28 of Directive 95/46.  
70      Article 12(b) of Directive 95/46 provides that Member States are to guarantee every data subject the right to obtain from the controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data. As this final point relating to the case where certain requirements referred to in Article 6(1)(d) of Directive 95/46 are not observed is stated by way of example and is not exhaustive, it follows that non-compliant nature of the processing, which is capable of conferring upon the data subject the right guaranteed in Article 12(b) of the directive, may also arise from non-observance of the other conditions of lawfulness that are imposed by the directive upon the processing of personal data.   
71      In this connection, it should be noted that, subject to the exceptions permitted under Article 13 of Directive 95/46, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (see   
Österreichischer Rundfunk and Others  
 EU:C:2003:294, paragraph 65; Joined Cases C-468/10 and C-469/10   
ASNEF and FECEMD  
 EU:C:2011:777, paragraph 26; and Case C-342/12   
Worten   
EU:C:2013:355, paragraph 33).  
72      Under Article 6 of Directive 95/46 and without prejudice to specific provisions that the Member States may lay down in respect of processing for historical, statistical or scientific purposes, the controller has the task of ensuring that personal data are processed ‘fairly and lawfully’, that they are ‘collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes’, that they are ‘adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed’, that they are ‘accurate and, where necessary, kept up to date’ and, finally, that they are ‘kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed’. In this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified.  
73      As regards legitimation, under Article 7 of Directive 95/46, of processing such as that at issue in the main proceedings carried out by the operator of a search engine, that processing is capable of being covered by the ground in Article 7(f).  
74      This provision permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy with respect to the processing of personal data — which require protection under Article 1(1) of the directive. Application of Article 7(f) thus necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject’s rights arising from Articles 7 and 8 of the Charter (see   
ASNEF and FECEMD  
, EU:C:2011:777, paragraphs 38 and 40).  
75      Whilst the question whether the processing complies with Articles 6 and 7(f) of Directive 95/46 may be determined in the context of a request as provided for in Article 12(b) of the directive, the data subject may, in addition, rely in certain conditions on the right to object laid down in subparagraph (a) of the first paragraph of Article 14 of the directive.  
76      Under subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, Member States are to grant the data subject the right, at least in the cases referred to in Article 7(e) and (f) of the directive, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. The balancing to be carried out under subparagraph (a) of the first paragraph of Article 14 thus enables account to be taken in a more specific manner of all the circumstances surrounding the data subject’s particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.  
77      Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.  
78      In this connection, it is to be noted that it is clear from Article 28(3) and (4) of Directive 95/46 that each supervisory authority is to hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data and that it has investigative powers and effective powers of intervention enabling it to order in particular the blocking, erasure or destruction of data or to impose a temporary or definitive ban on such processing.  
79      It is in the light of those considerations that it is necessary to interpret and apply the provisions of Directive 95/46 governing the data subject’s rights when he lodges with the supervisory authority or judicial authority a request such as that at issue in the main proceedings.  
80      It must be pointed out at the outset that, as has been found in paragraphs 36 to 38 of the present judgment, processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual’s name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10   
eDate Advertising and Others  
 EU:C:2011:685, paragraph 45).  
81      In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing. However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject’s fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject’s rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject’s private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.  
82      Following the appraisal of the conditions for the application of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 which is to be carried out when a request such as that at issue in the main proceedings is lodged with it, the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages published by third parties containing information relating to that person, without an order to that effect presupposing the previous or simultaneous removal of that name and information — of the publisher’s own accord or following an order of one of those authorities — from the web page on which they were published.  
83      As has been established in paragraphs 35 to 38 of the present judgment, inasmuch as the data processing carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites and affects the data subject’s fundamental rights additionally, the operator of the search engine as the controller in respect of that processing must ensure, within the framework of its responsibilities, powers and capabilities, that that processing meets the requirements of Directive 95/46, in order that the guarantees laid down by the directive may have full effect.  
84      Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.  
85      Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out ‘solely for journalistic purposes’ and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. It cannot therefore be ruled out that in certain circumstances the data subject is capable of exercising the rights referred to in Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 against that operator but not against the publisher of the web page.   
86      Finally, it must be stated that not only does the ground, under Article 7 of Directive 95/46, justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same.  
87      Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person’s name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject’s fundamental right to privacy than the publication on the web page.  
88      In the light of all the foregoing considerations, the answer to Question 2(c) and (d) is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.  
   
Question 3, concerning the scope of the data subject’s rights guaranteed by Directive 95/46  
89      By Question 3, the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as enabling the data subject to require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be ‘forgotten’ after a certain time.   
90      Google Spain, Google Inc., the Greek, Austrian and Polish Governments and the Commission consider that this question should be answered in the negative. Google Spain, Google Inc., the Polish Government and the Commission submit in this regard that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 confer rights upon data subjects only if the processing in question is incompatible with the directive or on compelling legitimate grounds relating to their particular situation, and not merely because they consider that that processing may be prejudicial to them or they wish that the data being processed sink into oblivion. The Greek and Austrian Governments submit that the data subject must approach the publisher of the website concerned.  
91      According to Mr Costeja González and the Spanish and Italian Governments, the data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy — which encompass the ‘right to be forgotten’ — override the legitimate interests of the operator of the search engine and the general interest in freedom of information.  
92      As regards Article 12(b) of Directive 95/46, the application of which is subject to the condition that the processing of personal data be incompatible with the directive, it should be recalled that, as has been noted in paragraph 72 of the present judgment, such incompatibility may result not only from the fact that such data are inaccurate but, in particular, also from the fact that they are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.  
93      It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.  
94      Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.  
95      So far as concerns requests as provided for by Article 12(b) of Directive 95/46 founded on alleged non-compliance with the conditions laid down in Article 7(f) of the directive and requests under subparagraph (a) of the first paragraph of Article 14 of the directive, it must be pointed out that in each case the processing of personal data must be authorised under Article 7 for the entire period during which it is carried out.  
96      In the light of the foregoing, when appraising such requests made in order to oppose processing such as that at issue in the main proceedings, it should in particular be examined whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. In this connection, it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject.  
97      As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, as follows in particular from paragraph 81 of the present judgment, that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject’s name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.  
98      As regards a situation such as that at issue in the main proceedings, which concerns the display, in the list of results that the internet user obtains by making a search by means of Google Search on the basis of the data subject’s name, of links to pages of the on-line archives of a daily newspaper that contain announcements mentioning the data subject’s name and relating to a real-estate auction connected with attachment proceedings for the recovery of social security debts, it should be held that, having regard to the sensitivity for the data subject’s private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed from the list of results.  
99      It follows from the foregoing considerations that the answer to Question 3 is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject’s name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.  
   
Costs  
100    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the ‘controller’ in respect of that processing, within the meaning of Article 2(d).  
2.        
Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.  
3.        
Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.   
4.        
Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject’s name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

ID: a5777b81-ea0a-43e2-9b00-f58e50fdda94

Judgment of 16 Dec 2008, C-524/06 (  
Huber  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Performance of a task of public interest or official authority   
   
JUDGMENT OF THE COURT (Grand Chamber)  
16 December 2008 (\*)  
(Protection of personal data – European citizenship – Principle of non-discrimination on grounds of nationality – Directive 95/46/EC – Concept of necessity – General processing of personal data relating to citizens of the Union who are nationals of another Member State – Central register of foreign nationals)  
In Case C-524/06,  
REFERENCE for a preliminary ruling under Article 234 EC from the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Germany), made by decision of 15 December 2006, received at the Court on 28 December 2006, in the proceedings  
Heinz Huber  
v  
Bundesrepublik Deutschland,  
THE COURT (Grand Chamber),  
composed of V. Skouris, President, P. Jann, C.W.A. Timmermans and K. Lenaerts, Presidents of Chambers, P. Kūris, G. Arestis, U. Lõhmus, E. Levits (Rapporteur) and L. Bay Larsen, Judges,  
Advocate General: M. Poiares Maduro,  
Registrar: B. Fülöp, Administrator,  
having regard to the written procedure and further to the hearing on 8 January 2008,  
after considering the observations submitted on behalf of:  
–        Mr Huber, by A. Widmann, Rechtsanwalt,  
–        the German Government, by M. Lumma and C. Schulze-Bahr, acting as Agents, and by Professor K. Hailbronner,   
–        the Belgian Government, by L. Van den Broeck, acting as Agent,  
–        the Danish Government, by B. Weis Fogh, acting as Agent,  
–        the Greek Government, by E.-M. Mamouna and K. Boskovits, acting as Agents,  
–        the Italian Government, by I.M. Braguglia, acting as Agent, and by W. Ferrante, avvocato dello Stato,  
–        the Netherlands Government, by H.G. Sevenster, C.M. Wissels and C. ten Dam, acting as Agents,  
–        the Finnish Government, by J. Heliskoski, acting as Agent,  
–        the United Kingdom Government, by E. O’Neill, acting as Agent, and J. Stratford, Barrister,  
–        the Commission of the European Communities, by C. Docksey and C. Ladenburger, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 3 April 2008,  
gives the following  
Judgment  
1        This reference for a preliminary ruling concerns Article 12(1) EC, read in conjunction with Articles 17 EC and 18 EC, the first paragraph of Article 43 EC, as well as Article 7(e) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).   
2        The reference was made in proceedings between Mr Huber, an Austrian national who is resident in Germany, and the Bundesrepublik Deutschland, represented by the Bundesamt für Migration und Flüchtlinge (Federal Office for Migration and Refugees) (‘the Bundesamt’), regarding Mr Huber’s request for the deletion of the data relating to him in the Central Register of Foreign Nationals (Ausländerzentralregister) (‘the AZR’).  
   
Legal context  
   
Community legislation  
3        The eighth recital in the preamble to Directive 95/46 states:  
‘Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; …’.  
4        The tenth recital in the preamble to that directive adds:  
‘… the approximation of [the national laws on the processing of personal data] must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community’.   
5        Article 1 of Directive 95/46 is entitled ‘Object of the Directive’ and Article 1(1) provides:  
‘In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.’  
6        Article 2 of that directive includes the following definitions:  
‘…  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;  
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…’.  
7        The scope of application of Directive 95/46 is laid down by Article 3, in the following terms:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
8        Article 7(e) of Directive 95/46 states:  
‘Member States shall provide that personal data may be processed only if:  
…  
(e)       processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;   
…’.  
9        Article 4 of Council Directive 68/360/EEC of 15 October 1968 on the abolition of restrictions on movement and residence within the Community for workers of Member States and their families (OJ, English Special Edition 1968 (II), p. 485) provides:  
‘1.      Member States shall grant the right of residence in their territory to the persons referred to in Article 1 who are able to produce the documents listed in paragraph 3.  
2.      As proof of the right of residence, a document entitled “Residence Permit for a National of a Member State of the EEC” shall be issued. …   
3.      For the issue of a Residence Permit for a National of a Member State of the EEC, Member States may require only the production of the following documents:  
–         by the worker:   
(a)      the document with which he entered their territory;  
(b)      a confirmation of engagement from the employer or a certificate of employment;  
–        by the members of the worker’s family:   
(c)      the document with which they entered the territory;  
(d)      a document issued by the competent authority of the State of origin or the State whence they came, proving their relationship;  
(e)      in the cases referred to in Article 10(1) and (2) of [Council Regulation (EEC) No 1612/68 of 15 October 1968 on freedom of movement for workers within the Community (OJ, English Special Edition 1968 (II), p. 475)], a document issued by the competent authority of the State of origin or the State whence they came, testifying that they are dependent on the worker or that they live under his roof in such country.  
…’  
10      Article 10 of Directive 68/360 provides:  
‘Member States shall not derogate from the provisions of this Directive save on grounds of public policy, public security or public health.’  
11      Article 4(1) of Council Directive 73/148/EEC of 21 May 1973 on the abolition of restrictions on movement and residence within the Community for nationals of Member States with regard to establishment and the provision of services (OJ 1973 L 172, p. 14) states:  
‘Each Member State shall grant the right of permanent residence to nationals of other Member States who establish themselves within its territory in order to pursue activities as self-employed persons, when the restrictions on these activities have been abolished pursuant to the Treaty.  
As proof of the right of residence, a document entitled “Residence Permit for a National of a Member State of the European Communities” shall be issued. This document shall be valid for not less than five years from the date of issue and shall be automatically renewable.  
…’  
12      Article 6 of Directive 73/148 states:  
‘An applicant for a residence permit or right of abode shall not be required by a Member State to produce anything other than the following, namely:  
(a)      the identity card or passport with which he or she entered its territory;  
(b)      proof that he or she comes within one of the classes of person referred to in Articles 1 and 4.’  
13      Article 8 of that directive sets out the derogation provided for in Article 10 of Directive 68/360.   
14      On 29 April 2004, the European Parliament and the Council of the European Union adopted Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ 2004 L 158, p. 77, with Corrigendum, OJ 2004 L 229, p. 35), which required to be transposed by 30 April 2006. Article 5 of that directive provides:   
‘1.      Without prejudice to the provisions on travel documents applicable to national border controls, Member States shall grant Union citizens leave to enter their territory with a valid identity card or passport and shall grant family members who are not nationals of a Member State leave to enter their territory with a valid passport.  
…  
5.      The Member State may require the person concerned to report his/her presence within its territory within a reasonable and non-discriminatory period of time. Failure to comply with this requirement may make the person concerned liable to proportionate and non-discriminatory sanctions.’  
15      Article 7(1) of that directive governs the right of residence for a period of more than three months of Union citizens in a Member State of which they are not nationals in the following terms:  
‘All Union citizens shall have the right of residence on the territory of another Member State for a period of longer than three months if they:  
(a)      are workers or self-employed persons in the host Member State; or   
(b)      have sufficient resources for themselves and their family members not to become a burden on the social assistance system of the host Member State during their period of residence and have comprehensive sickness insurance cover in the host Member State; or   
(c)      –       are enrolled at a private or public establishment, accredited or financed by the host Member State on the basis of its legislation or administrative practice, for the principal purpose of following a course of study, including vocational training; and  
         –       have comprehensive sickness insurance cover in the host Member State and assure the relevant national authority, by means of a declaration or by such equivalent means as they may choose, that they have sufficient resources for themselves and their family members not to become a burden on the social assistance system of the host Member State during their period of residence; or  
…’.  
16      Article 8 of Directive 2004/38 provides:   
‘1.      Without prejudice to Article 5(5), for periods of residence longer than three months, the host Member State may require Union citizens to register with the relevant authorities.  
2.      The deadline for registration may not be less than three months from the date of arrival. A registration certificate shall be issued immediately, stating the name and address of the person registering and the date of the registration. Failure to comply with the registration requirement may render the person concerned liable to proportionate and non-discriminatory sanctions.  
3.      For the registration certificate to be issued, Member States may only require that:  
–        Union citizens to whom point (a) of Article 7(1) applies present a valid identity card or passport, a confirmation of engagement from the employer or a certificate of employment, or proof that they are self-employed persons;  
–        Union citizens to whom point (b) of Article 7(1) applies present a valid identity card or passport and provide proof that they satisfy the conditions laid down therein;  
–        Union citizens to whom point (c) of Article 7(1) applies present a valid identity card or passport, provide proof of enrolment at an accredited establishment and of comprehensive sickness insurance cover and the declaration or equivalent means referred to in point (c) of Article 7(1). …’  
17      Article 27 of that directive, entitled ‘General principles’, states:   
‘1.      Subject to the provisions of this Chapter, Member States may restrict the freedom of movement and residence of Union citizens and their family members, irrespective of nationality, on grounds of public policy, public security or public health. These grounds shall not be invoked to serve economic ends.  
2.      Measures taken on grounds of public policy or public security shall comply with the principle of proportionality and shall be based exclusively on the personal conduct of the individual concerned. Previous criminal convictions shall not in themselves constitute grounds for taking such measures.  
The personal conduct of the individual concerned must represent a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society. Justifications that are isolated from the particulars of the case or that rely on considerations of general prevention shall not be accepted.  
3.      In order to ascertain whether the person concerned represents a danger for public policy or public security, when issuing the registration certificate or, in the absence of a registration system, not later than three months from the date of arrival of the person concerned on its territory or from the date of reporting his/her presence within the territory, as provided for in Article 5(5), or when issuing the residence card, the host Member State may, should it consider this essential, request the Member State of origin and, if need be, other Member States to provide information concerning any previous police record the person concerned may have. Such enquiries shall not be made as a matter of routine. …  
…’  
18      Lastly, Regulation (EC) No 862/2007 of the European Parliament and of the Council of 11 July 2007 on Community statistics on migration and international protection and repealing Council Regulation (EEC) No 311/76 on the compilation of statistics on foreign workers (OJ 2007 L 199, p. 23) lays down the framework in which the Member States are to supply statistics to the Commission of the European Communities relating to migratory flows in their territories.   
   
National legislation  
19      In accordance with Paragraph 1(1) of the Law on the central register of foreign nationals (Gesetz über das Ausländerzentralregister) of 2 September 1994 (BGBl. 1994 I, p. 2265), as amended by the Law of 21 June 2005 (BGBl. 1994 I, p. 1818) (‘the AZRG’), the Bundesamt, which is attached to the Federal Ministry of the Interior, is responsible for the management of the AZR, a centralised register which contains certain personal data relating to foreign nationals who, inter alia, are resident in Germany on a basis which is not purely temporary. The foreign nationals concerned are those who reside in that territory for a period of more than three months, as is shown by the general administrative circular of the Federal Ministry of the Interior relating to the AZRG and to the regulation implementing that Law (Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum Gesetz über das AZR und zur AZRG-Durchführungsverordnung) of 4 June 1996. That information is collected in two databases which are managed separately. One contains personal data relating to foreign nationals who live or have lived in Germany and the other to those who have applied for a visa.  
20      In accordance with Paragraph 3 of the AZRG, the first database contains, in particular, the following information:   
–        the name of the authority which provided the data;  
–        the reference number allocated by the Bundesamt;  
–        the grounds of registration;   
–        surname, surname at birth, given names, date and place of birth, sex and nationality;   
–        previous and other patronymics, marital status, particulars of identity documents, the last place of residence in the country of origin, and information supplied on a voluntary basis as to religion and the nationality of the spouse or partner;   
–        particulars of entries into and exits from the territory, residence status, decisions of the Federal Employment Agency relating to a work permit, refugee status granted by another State, date of death;  
–        decisions relating, inter alia, to any application for asylum, any previous application for a residence permit, and particulars of, inter alia, any expulsion proceedings, arrest warrants, suspected contraventions of the laws on drugs or immigration, and suspected participation in terrorist activities, or convictions in respect of such activities; and  
–        search warrants.  
21      As the authority entrusted with the management of the AZR, the Bundesamt is responsible for the accuracy of the data registered in it.  
22      According to Paragraph 1(2) of the AZRG, by registering and supplying personal data relating to foreign nationals, the Bundesamt assists the public authorities responsible for the application of the law on foreign nationals and the law on asylum, together with other public bodies.   
23      Paragraph 10(1) of the AZRG provides that every application made by a public authority to consult the AZR or for the making available of personal data contained in it must satisfy certain conditions, compliance with which must be determined by the Bundesamt on a case-by-case basis. The Bundesamt must, in particular, examine whether the data requested by an authority are necessary for the performance of its tasks and must also examine the precise use to which those data are intended to be put. The Bundesamt may reject an application if it does not satisfy the prescribed conditions.  
24      Paragraphs 14 to 21 and 25 to 27 of the Law specify the personal data which may be made available depending on the body which made the application in respect of them.  
25      Thus, Paragraph 14(1) of the AZRG authorises the communication to all German public authorities of data relating to identity and domicile, as well as the date of death and particulars of the authority responsible for the file and of any decision not to make data available.  
26      Paragraph 12 of the AZRG provides that applications, termed ‘group applications’, that is to say, which relate to a group of persons having one or more common characteristics, are to be subject to certain substantive and formal conditions. Such applications may be made only by a limited number of public bodies. In addition, every communication of personal data pursuant to such an application must be notified to the Federal and regional regulators responsible for the protection of personal data.  
27      In addition, Paragraph 22 of the AZRG permits public bodies authorised for that purpose to consult the AZR directly through an automated procedure. However, the right to do so arises only in strictly defined circumstances and after a weighing up by the Bundesamt of the interests of the data subject and the public interest. Moreover, such consultation is allowed only in the case of so-called group applications. The public bodies having rights under Paragraph 22 of the AZRG are, by virtue of Paragraph 7 of that Law, also authorised to enter data and information directly in the AZR.  
28      Lastly, Paragraphs 25 to 27 of the AZRG specify the public bodies which may obtain certain data contained in the AZR.  
29      The national court adds that, in Germany, every inhabitant, whether a German national or not, must have his particulars entered in the register kept by the authorities of the district in which he resides (Einwohnermelderegister). The Commission has stated in that regard that that type of register contains only some of the data comprised in the AZR, with those relating, in particular, to a person’s status as regards his right of residence not appearing there. There are currently some 7 700 district registers.  
   
The facts and the questions referred   
30      Mr Huber, an Austrian national, moved to Germany in 1996 in order to carry on business there as a self-employed insurance agent.   
31      The following data relating to him are stored in the AZR:  
–        his name, given name, date and place of birth, nationality, marital status, sex;  
–        a record of his entries into and exits from Germany, and his residence status;  
–        particulars of passports issued to him;  
–        a record of his previous statements as to domicile; and  
–        reference numbers issued by the Bundesamt, particulars of the authorities which supplied the data and the reference numbers used by those authorities.  
32      Since he took the view that he was discriminated against by reason of the processing of the data concerning him contained in the AZR, in particular because such a database does not exist in respect of German nationals, Mr Huber requested the deletion of those data on 22 July 2000. That request was rejected on 29 September 2000 by the administrative authority which was responsible for maintaining the AZR at the time.  
33      The challenge to that decision also having been unsuccessful, Mr Huber brought an action before the Verwaltungsgericht Köln (Administrative Court, Cologne) which upheld the action by judgment of 19 December 2002. The Verwaltungsgericht Köln held that the general processing, through the AZR, of data regarding a Union citizen who is not a German national constitutes a restriction of Articles 49 EC and 50 EC which cannot be justified by the objective of the swift treatment of cases relating to the right of residence of foreign nationals. In addition, that court took the view that the storage and processing of the data at issue were contrary to Articles 12 EC and 18 EC, as well as Articles 6(1)(b) and 7(e) of Directive 95/46.  
34      The Bundesrepublik Deutschland, acting through the Bundesamt, brought an appeal against that judgment before the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Higher Administrative Court for the   
Land   
North-Rhine Westphalia), which considers that certain of the questions of law raised before it require an interpretation of Community law by the Court.  
35      First, the national court notes that, according to the Court’s case-law, a citizen of the European Union lawfully resident in the territory of a Member State of which he is not a national can rely on Article 12 EC in all situations which fall within the scope of Community law. It refers in that regard to Case C-85/96   
Martínez Sala   
[1998] ECR I-2691, paragraph 63; Case C-184/99   
Grzelczyk  
 [2001] ECR I-6193, paragraph 32; and Case C-209/03   
Bidar   
[2005] ECR I-2119, paragraph 32. Accordingly, having exercised the right to the freedom of movement conferred on him by Article 18(1) EC, Mr Huber was entitled to rely on the prohibition of discrimination laid down by Article 12 EC.  
36      The national court states that the general processing of personal data relating to Mr Huber in the AZR differs from the processing of data relating to a German national in two respects: first, some of the data relating to Mr Huber are stored not only in the register of the district in which he resides but also in the AZR, and, secondly, the AZR contains additional data.   
37      The national court doubts whether such a difference in treatment can be justified by the need to monitor the residence of foreign nationals in Germany. It also raises the question whether the general processing of personal data relating to Union citizens who are not German nationals and who reside or have resided in Germany is proportionate to the objective of protecting public security, inasmuch as the AZR covers all of those citizens and not only those who are subject to an expulsion order or a prohibition on residing in Germany.  
38      Secondly, the national court is of the opinion that, in the circumstances of the main proceedings, Mr Huber falls within the scope of application of Article 43 EC. Since the freedom of establishment extends not only to the taking up of activities as a self-employed person but also the framework conditions for that activity, the national court raises the question whether the general processing of data relating to Mr Huber in the AZR is liable to affect those conditions to such an extent that it comprises a restriction on the exercise of that freedom.  
39      Thirdly, the national court raises the question whether the criterion of necessity imposed by Article 7(e) of Directive 95/46 can be a criterion for assessing a system of general data processing such as the system put in place under the AZR. The national court does not, in fact, rule out the possibility that the directive may leave it open to the national legislature itself to define that requirement of necessity. However, should that not be the case, the question arises how that requirement is to be understood, and more particularly whether the objective of administrative simplification might justify data processing of the kind put in place by the AZRG.  
40      In those circumstances, the Oberverwaltungsgericht für das Land Nordrhein-Westfalen decided to stay the proceedings and refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is the general processing of personal data of foreign citizens of the Union in a central register of foreign nationals compatible with … the prohibition of discrimination on grounds of nationality against citizens of the Union who exercise their right to move and reside freely within the territory of the Member States (Article 12(1) EC, in conjunction with Articles 17 EC and 18(1) EC)[?]  
(2)      [Is such processing compatible with] the prohibition of restrictions on the freedom of establishment of nationals of a Member State in the territory of another Member State (first paragraph of Article 43 EC)[?]  
(3)       [Is such treatment compatible with] the requirement of necessity under Article 7(e) of Directive 95/46 …?’  
   
The questions referred  
   
Preliminary observations  
41      By its questions, the national court asks the Court whether the processing of personal data which is undertaken in a register such as the AZR is compatible with Community law.   
42      In that regard, it must be noted that Paragraph 1(2) of the AZRG provides that, through the storage of certain personal data relating to foreign nationals in the AZR and the making available of those data, the Bundesamt, which is responsible for maintaining that register, assists the public authorities responsible for the application of the legislation relating to the law on foreign nationals and the law on asylum, together with other public bodies. In particular, the German Government has stated in its written observations that the AZR is used for statistical purposes and on the exercise by the security and police services and by the judicial authorities of their powers in relation to the prosecution and investigation of activities which are criminal or threaten public security.   
43      At the outset, it must be stated that data such as those which, according to the order for reference, the AZR contains in relation to Mr Huber constitute personal data within the meaning of Article 2(a) of Directive 95/46, because they represent ‘information relating to an identified or identifiable natural person’. Their collection, storage and transmission by the body responsible for the management of the register in which they are kept thus represents the ‘processing of personal data’ within the meaning of Article 2(b) of that directive.  
44      However, Article 3(2) of Directive 95/46 expressly excludes from its scope of application, inter alia, the processing of personal data concerning public security, defence, State security and the activities of the State in areas of criminal law.  
45      It follows that, while the processing of personal data for the purposes of the application of the legislation relating to the right of residence and for statistical purposes falls within the scope of application of Directive 95/46, the position is otherwise where the objective of processing those data is connected with the fight against crime.  
46      Consequently, the compatibility with Community law of the processing of personal data undertaken through a register such as the AZR should be examined, first, in the context of its function of providing support to the authorities responsible for the application of the legislation relating to the right of residence and to its use for statistical purposes, by having regard to Directive 95/46 and more particularly, in view of the third question, to the condition of necessity laid down by Article 7(e) of that directive, as interpreted in the light of the requirements of the Treaty including in particular the prohibition of any discrimination on grounds of nationality under Article 12(1) EC, and, secondly, in the context of its function in the fight against crime, by having regard to primary Community law.  
   
The processing of personal data for the purpose of the application of the legislation relating to the right of residence and for statistical purposes   
 The concept of necessity   
47      Article 1 of Directive 95/46 requires Member States to ensure the protection of the fundamental rights and freedoms of natural persons, and in particular their privacy, in relation to the handling of personal data.  
48      Chapter II of Directive 95/46, entitled ‘General rules on the lawfulness of the processing of personal data’, provides that, subject to the exceptions permitted under Article 13, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 (see, to that effect, Joined Cases C-465/00, C-138/01 and C-139/01   
Österreichischer Rundfunk and Others   
[2003] ECR I-4989, paragraph 65).  
49      In particular, Article 7(e) provides that personal data may lawfully be processed if ‘it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed’.  
50      In that context, it must be noted that Directive 95/46 is intended, as appears from the eighth recital in the preamble thereto, to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. The tenth recital adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.  
51      Thus, it has been held that the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete (see Case C-101/01   
Lindqvist  
 [2003] ECR I-12971, paragraph 96).  
52      Consequently, having regard to the objective of ensuring an equivalent level of protection in all Member States, the concept of necessity laid down by Article 7(e) of Directive 95/46, the purpose of which is to delimit precisely one of the situations in which the processing of personal data is lawful, cannot have a meaning which varies between the Member States. It therefore follows that what is at issue is a concept which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that directive, as laid down in Article 1(1) thereof.  
 The necessity for the processing of personal data, such as the processing undertaken through the AZR, for the purpose of the application of the legislation relating to the right of residence and for statistical purposes   
53      It is apparent from the order for reference that the AZR is a centralised register which contains certain personal data relating to Union citizens who are not German nationals and that it may be consulted by a number of public and private bodies.   
54      As regards the use of a register such as the AZR for the purpose of the application of the legislation relating to the right of residence, it is important to bear in mind that, as Community law presently stands, the right of free movement of a Union citizen in the territory of a Member State of which he is not a national is not unconditional but may be subject to the limitations and conditions imposed by the Treaty and by the measures adopted to give it effect (see, to that effect, Case C-33/07   
Jippa   
[2008] ECR I-0000, paragraph 21 and the case-law cited).  
55      Thus, Article 4 of Directive 68/360, read in conjunction with Article 1 thereof, and Article 6 of Directive 73/148, read in conjunction with Article 1 thereof, provided that, in order for a national of a Member State to be entitled to reside for a period of more than three months in the territory of another Member State, that person had to belong to one of the categories laid down by those directives and provided for that entitlement to be subject to certain formalities linked to the presentation or the provision by the applicant of a residence permit together with various documents and particulars.  
56      In addition, Article 10 of Directive 68/360 and Article 8 of Directive 73/148 permitted Member States to derogate from the provisions of those directives on grounds of public policy, public security or public health and to limit the right of entry and residence of a national of another Member State in their territory.  
57      While Directive 2004/38, which fell to be transposed by 30 April 2006 and which accordingly did not apply at the time of the facts of the present case, repealed both of the abovementioned directives, it sets out, in Article 7, conditions which are generally equivalent to those laid down under its predecessors as regards the right of residence of nationals of other Member States and, in Article 27(1), restrictions relating to that right which are essentially identical to those laid down under its predecessors. It also provides, in Article 8(1), that the host Member State may require every Union citizen who is a national of another Member State and who wishes to reside in its territory for a period of more than three months to register with the relevant authorities. In that regard, the host Member State may, by virtue of Article 8(3), require certain documents and particulars to be provided in order to enable those authorities to determine that the conditions for entitlement to a right of residence are satisfied.  
58      It must therefore be held that it is necessary for a Member State to have the relevant particulars and documents available to it in order to ascertain, within the framework laid down under the applicable Community legislation, whether a right of residence in its territory exists in relation to a national of another Member State and to establish that there are no grounds which would justify a restriction on that right. It follows that the use of a register such as the AZR for the purpose of providing support to the authorities responsible for the application of the legislation relating to the right of residence is, in principle, legitimate and, having regard to its nature, compatible with the prohibition of discrimination on grounds of nationality laid down by Article 12(1) EC.  
59      However, such a register must not contain any information other than what is necessary for that purpose. In that regard, as Community law presently stands, the processing of personal data contained in the documents referred to in Articles 8(3) and 27(1) of Directive 2004/38 must be considered to be necessary, within the meaning of Article 7(e) of Directive 95/46, for the application of the legislation relating to the right of residence.  
60      Moreover, while the collection of the data required for the application of the legislation relating to the right of residence would be of no practical benefit if those data were not to be stored, it must be emphasised that, since a change in the personal situation of a party entitled to a right of residence may have an impact on his status in relation to that right, it is incumbent on the authority responsible for a register such as the AZR to ensure that the data which are stored are, where appropriate, brought up to date so that, first, they reflect the actual situation of the data subjects and, secondly, irrelevant data are removed from that register.  
61      As regards the detailed rules for the use of such a register for the purposes of the application of the legislation relating to the right of residence, only the grant of access to authorities having powers in that field could be considered to be necessary within the meaning of Article 7(e) of Directive 95/46.  
62      Lastly, with respect to the necessity that a centralised register such as the AZR be available in order to meet the requirements of the authorities responsible for the application of the legislation relating to the right of residence, even if it were to be assumed that decentralised registers such as the district population registers contain all the data which are relevant for the purposes of allowing the authorities to undertake their duties, the centralisation of those data could be necessary, within the meaning of Article 7(e) of Directive 95/46, if it contributes to the more effective application of that legislation as regards the right of residence of Union citizens who wish to reside in a Member State of which they are not nationals.   
63      As regards the statistical function of a register such as the AZR, it must be recalled that, by creating the principle of freedom of movement for persons and by conferring on any person falling within its ambit the right of access to the territory of the Member States for the purposes intended by the Treaty, Community law has not excluded the power of Member States to adopt measures enabling the national authorities to have an exact knowledge of population movements affecting their territory (see Case 118/75   
Watson and Belmann   
[1976] ECR 1185, paragraph 17).  
64      Similarly, Regulation No 862/2007, which provides for the transmission of statistics relating to migratory flows in the territory of the Member States, presupposes that information will be collected by those States which allows those statistics to be determined.  
65      However, the exercise of that power does not, of itself, mean that the collection and storage of individualised personal information in a register such as the AZR is necessary, within the meaning of Article 7(e) of Directive 95/46. As the Advocate General stated at point 23 of his Opinion, it is only anonymous information that requires to be processed in order for such an objective to be attained.  
66      It follows from all of the above that a system for processing personal data relating to Union citizens who are not nationals of the Member State concerned, such as that put in place by the AZRG and having as its object the provision of support to the national authorities responsible for the application of the legislation relating to the right of residence, does not satisfy the requirement of necessity laid down by Article 7(e) of Directive 95/46, interpreted in the light of the prohibition on any discrimination on grounds of nationality, unless:  
–        it contains only the data which are necessary for the application by those authorities of that legislation, and  
–        its centralised nature enables that legislation to be more effectively applied as regards the right of residence of Union citizens who are not nationals of that Member State.  
67      It is for the national court to ascertain whether those conditions are satisfied in the main proceedings.  
68      The storage and processing of personal data containing individualised personal information in a register such as the AZR for statistical purposes cannot, on any basis, be considered to be necessary within the meaning of Article 7(e) of Directive 95/46.  
   
The processing of personal data relating to Union citizens who are nationals of other Member States for the purposes of fighting crime   
69      As a preliminary point, it should be noted that, according to settled case-law, citizenship of the Union is destined to be the fundamental status of nationals of the Member States, enabling those who find themselves in the same situation to receive the same treatment in law irrespective of their nationality, subject to such exceptions as are expressly provided for (see, to that effect,   
Grzelczyk  
, paragraphs 30 and 31; Case C-148/02   
Garcia Avello   
[2003] ECR I-11613, paragraphs 22 and 23; and   
Bidar  
, paragraph 31).  
70      In that regard, a Union citizen lawfully resident in the territory of the host Member State can rely on Article 12 EC in all situations which fall within the scope ratione materiae of Community law (see   
Martínez Sala  
, paragraph 63;   
Grzelczyk  
, paragraph 32; and   
Bidar  
, paragraph 32).  
71      Those situations include those involving the exercise of the fundamental freedoms guaranteed by the Treaty and those involving the exercise of the right to move and reside within the territory of the Member States, as conferred by Article 18 EC (see, to that effect,   
Bidar  
, paragraph 33 and the case-law cited).  
72      It is apparent from Paragraph 1 of the AZRG, read in conjunction with the general administrative circular of the Federal Ministry of the Interior of 4 June 1996 relating to the AZRG and to the regulation implementing that Law, that the system of storage and processing of personal data put in place through the AZR concerns all Union citizens who are not nationals of the Federal Republic of Germany and who reside in Germany for a period of over three months, irrespective of the reasons which lead them to reside there.  
73      That being the case, since Mr Huber exercised his freedom to move and reside within that territory as conferred by Article 18 EC, reference should, having regard to the circumstances of the main proceedings, be made to Article 12(1) EC in order to determine whether a system for the storage and processing of personal data such as that at issue in the main proceedings is compatible with the principle that any discrimination on grounds of nationality is prohibited, in so far as those data are stored and processed for the purposes of fighting crime.  
74      In that context, it should be pointed out that the order for reference does not contain any detailed information which would allow it to be established whether the situation at issue in the main proceedings is covered by Article 43 EC. However, even if the national court were to consider that to be the case, the application of the principle of non-discrimination cannot vary depending on whether it finds its basis in that provision or on Article 12(1) EC, read in conjunction with Article 18(1) EC.   
75      It is settled case-law that the principle of non-discrimination, which has its basis in Articles 12 EC and 43 EC, requires that comparable situations must not be treated differently and that different situations must not be treated in the same way. Such treatment may be justified only if it is based on objective considerations independent of the nationality of the persons concerned and is proportionate to the objective being legitimately pursued (see, to that effect, Case C-164/07   
Wood   
[2008] ECR I-0000, paragraph 13 and the case-law cited).  
76      It is therefore, in circumstances such as those at issue in the main proceedings, necessary to compare the situation of Union citizens who are not nationals of the Member State concerned and who are resident in the territory of that Member State with that of nationals of that Member State as regards the objective of fighting crime. In fact, the German Government relies only on that aspect of the protection of public order.  
77      Although that objective is a legitimate one, it cannot be relied on in order to justify the systematic processing of personal data when that processing is restricted to the data of Union citizens who are not nationals of the Member State concerned.  
78      As the Advocate General noted at point 21 of his Opinion, the fight against crime, in the general sense in which that term is used by the German Government in its observations, necessarily involves the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators.  
79      It follows that, as regards a Member State, the situation of its nationals cannot, as regards the objective of fighting crime, be different from that of Union citizens who are not nationals of that Member State and who are resident in its territory.  
80      Therefore, the difference in treatment between those nationals and those Union citizens which arises by virtue of the systematic processing of personal data relating only to Union citizens who are not nationals of the Member State concerned for the purposes of fighting crime constitutes discrimination which is prohibited by Article 12(1) EC.  
81      Consequently, Article 12(1) EC must be interpreted as meaning that it precludes the putting in place by a Member State, for the purpose of fighting crime, of a system for processing personal data specific to Union citizens who are not nationals of that Member State.  
   
Costs  
82      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
A system for processing personal data relating to Union citizens who are not nationals of the Member State concerned, such as that put in place by the Law on the central register of foreign nationals (Gesetz über das Ausländerzentralregister) of 2 September 1994, as amended by the Law of 21 June 2005, and having as its object the provision of support to the national authorities responsible for the application of the law relating to the right of residence does not satisfy the requirement of necessity laid down by Article 7(e) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, interpreted in the light of the prohibition on any discrimination on grounds of nationality, unless:  
–          
it contains only the data which are necessary for the application by those authorities of that legislation, and   
–          
its centralised nature enables the legislation relating to the right of residence to be more effectively applied as regards Union citizens who are not nationals of that Member State.  
It is for the national court to ascertain whether those conditions are satisfied in the main proceedings.  
The storage and processing of personal data containing individualised personal information in a register such as the Central Register of Foreign Nationals for statistical purposes cannot, on any basis, be considered to be necessary within the meaning of Article 7(e) of Directive 95/46.  
2.        
Article 12(1) EC must be interpreted as meaning that it precludes the putting in place by a Member State, for the purpose of fighting crime, of a system for processing personal data specific to Union citizens who are not nationals of that Member State.

ID: a7a1a32d-1bab-4945-b929-d7fd993a1b52

Judgment of 22 Nov 2022, C-37/20 (  
Luxembourg Business Registers  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
   
JUDGMENT OF THE COURT (Grand Chamber)  
22 November 2022 (\*)  
(Reference for a preliminary ruling – Prevention of the use of the financial system for the purposes of money laundering or terrorist financing – Directive (EU) 2018/843 amending Directive (EU) 2015/849 – Amendment to Article 30(5), first subparagraph, point (c), of Directive 2015/849 – Access for any member of the general public to the information on beneficial ownership – Validity – Articles 7 and 8 of the Charter of Fundamental Rights of the European Union – Respect for private and family life – Protection of personal data)  
In Joined Cases C-37/20 and C-601/20,  
TWO REQUESTS for a preliminary ruling under Article 267 TFEU from the tribunal d’arrondissement de Luxembourg (Luxembourg District Court, Luxembourg), made by decisions of 24 January 2020 and 13 October 2020, received at the Court on 24 January 2020 and 13 November 2020 respectively, in the proceedings  
WM  
 (C-37/20),  
Sovim SA  
 (C-601/20)  
v  
Luxembourg Business Registers,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, K. Jürimäe, C. Lycourgos, E. Regan, M. Safjan, P.G. Xuereb, L.S. Rossi, Presidents of Chambers, S. Rodin, F. Biltgen, N. Piçarra, I. Jarukaitis, A. Kumin (Rapporteur) and I. Ziemele, Judges,  
Advocate General: G. Pitruzzella,  
Registrar: L. Carrasco Marco, Administrator,  
having regard to the written procedure and further to the hearing on 19 October 2021,  
after considering the observations submitted on behalf of:  
–        WM, by M. Jammaers, A. Komninos, L. Lorang and V. Staudt, avocats,  
–        Sovim SA, by P. Elvinger and K. Veranneman, avocats,  
–        the Luxembourg Government, by A. Germeaux, C. Schiltz and T. Uri, acting as Agents,  
–        the Austrian Government, by M. Augustin, A. Posch and J. Schmoll, acting as Agents,  
–        the Finnish Government, by M. Pere, acting as Agent,  
–        the Norwegian Government, by J.T. Kaasin and G. Østerman Thengs, acting as Agents,  
–        the European Parliament, by J. Etienne, O. Hrstková Šolcová and M. Menegatti, acting as Agents,  
–        the Council of the European Union, by M. Chavrier, I. Gurov and K. Pleśniak, acting as Agents,  
–        the European Commission, by V. Di Bucci, C. Giolito, L. Havas, H. Kranenborg, D. Nardi, T. Scharf and H. Tserepa-Lacombe, acting as Agents,  
–        the European Data Protection Supervisor, by C.-A. Marnier, acting as Agent,  
after hearing the Opinion of the Advocate General at the sitting on 20 January 2022,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern, in essence, the validity of Article 1(15)(c) of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ 2018 L 156, p. 43), in so far as Article 1(15)(c) amended point (c) of the first subparagraph of Article 30(5) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ 2015 L 141, p. 73), and also the interpretation, first, of Article 30(9) of Directive 2015/849, as amended by Directive 2018/843 (‘Directive 2015/849 as amended’), and, secondly, of Article 5(1)(a) to (c) and (f), Article 25(2) and Articles 44 to 50 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
2        The requests have been made in two sets of proceedings, the first between WM and Luxembourg Business Registers (‘LBR’) (Case C-37/20) and the second between Sovim SA and LBR (Case C-601/20), concerning LBR’s refusal to prevent the general public’s access to information concerning, first, WM’s status as the beneficial owner of a real estate company and, secondly, Sovim’s beneficial owner.  
   
Legal context  
   
European Union law  
   
Directives 2015/849, 2018/843, and 2015/849 as amended  
3        Recitals 4, 30, 31, 34, 36 and 38 of Directive 2018/843 state:  
‘(4)      … [it is necessary] to further increase the overall transparency of the economic and financial environment of the Union … The prevention of money laundering and of terrorist financing cannot be effective unless the environment is hostile to criminals seeking shelter for their finances through non-transparent structures. The integrity of the Union financial system is dependent on the transparency of corporate and other legal entities, trusts and similar legal arrangements. This Directive aims not only to detect and investigate money laundering, but also to prevent it from occurring. Enhancing transparency could be a powerful deterrent.  
…  
(30)      Public access to beneficial ownership information allows greater scrutiny of information by civil society, including by the press or civil society organisations, and contributes to preserving trust in the integrity of business transactions and of the financial system. It can contribute to combating the misuse of corporate and other legal entities and legal arrangements for the purposes of money laundering or terrorist financing, both by helping investigations and through reputational effects, given that anyone who could enter into transactions is aware of the identity of the beneficial owners. It also facilitates the timely and efficient availability of information for financial institutions as well as authorities, including authorities of third countries, involved in combating such offences. The access to that information would also help investigations on money laundering, associated predicate offences and terrorist financing.  
(31)      Confidence in financial markets from investors and the general public depends in large part on the existence of an accurate disclosure regime that provides transparency in the beneficial ownership and control structures of companies. … The potential increase in confidence in financial markets should be regarded as a positive side effect and not the purpose of increasing transparency, which is to create an environment less likely to be used for the purposes of money laundering and terrorist financing.  
…  
(34)      In all cases, both with regard to corporate and other legal entities, as well as trusts and similar legal arrangements, a fair balance should be sought in particular between the general public interest in the prevention of money laundering and terrorist financing and the data subjects’ fundamental rights. The set of data to be made available to the public should be limited, clearly and exhaustively defined, and should be of a general nature, so as to minimise the potential prejudice to the beneficial owners. At the same time, information made accessible to the public should not significantly differ from the data currently collected. In order to limit the interference with the right to respect for their private life in general and to protection of their personal data in particular, that information should relate essentially to the status of beneficial owners of corporate and other legal entities and of trusts and similar legal arrangements and should strictly concern the sphere of economic activity in which the beneficial owners operate. …  
…  
(36)      Moreover, with the aim of ensuring a proportionate and balanced approach and to guarantee the rights to private life and personal data protection, it should be possible for Member States to provide for exemptions to the disclosure through the registers of beneficial ownership information and to access to such information, in exceptional circumstances, where that information would expose the beneficial owner to a disproportionate risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation. It should also be possible for Member States to require online registration in order to identify any person who requests information from the register, as well as the payment of a fee for access to the information in the register.  
…  
(38)      [The GDPR] applies to the processing of personal data under this Directive. As a consequence, natural persons whose personal data are held in national registers as beneficial owners should be informed accordingly. Furthermore, only personal data that is up to date and corresponds to the actual beneficial owners should be made available and the beneficiaries should be informed about their rights under the current Union legal data protection framework … and the procedures applicable for exercising those rights. In addition, to prevent the abuse of the information contained in the registers and to balance out the rights of beneficial owners, Member States might find it appropriate to consider making information relating to the requesting person along with the legal basis for their request available to the beneficial owner.’  
4        Article 1(1) of Directive 2015/849 as amended provides:  
‘This Directive aims to prevent the use of the Union’s financial system for the purposes of money laundering and terrorist financing.’  
5        Article 3 of Directive 2015/849 as amended is worded:  
‘For the purposes of this Directive, the following definitions apply:  
…  
(6)      “beneficial owner” means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:  
(a)      in the case of corporate entities:  
(i)      the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity …  
…  
(ii)      if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), …  
…’  
6        Article 30(1) and (3) of Directive 2015/849 as amended provides:  
‘1.      Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held.  
…  
3.      Member States shall ensure that the information referred to in paragraph 1 is held in a central register in each Member State …  
…’  
7        In the version prior to the entry into force of Directive 2018/843, Article 30(5) and (9) of Directive 2015/849 was worded as follows:  
‘5.      Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:  
(a)      competent authorities and [Financial Intelligence Units], without any restriction;  
(b)      obliged entities, within the framework of customer due diligence in accordance with Chapter II;  
(c)      any person or organisation that can demonstrate a legitimate interest.  
The persons or organisations referred to in point (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held.  
…  
9.      Member States may provide for an exemption to the access referred to in points (b) and (c) of paragraph 5 to all or part of the information on the beneficial ownership on a case-by-case basis in exceptional circumstances, where such access would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, violence or intimidation, or where the beneficial owner is a minor or otherwise incapable. …’  
8        Article 1(15)(c), (d) and (g) of Directive 2018/843 amended paragraph 5, inserted a paragraph 5a and amended paragraph 9, respectively, of Article 30 of Directive 2015/849. Article 30(5), (5a) and (9) of Directive 2015/849 as amended therefore states:  
‘5.      Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:  
(a)      competent authorities and [Financial Intelligence Units], without any restriction;  
(b)      obliged entities, within the framework of customer due diligence in accordance with Chapter II;  
(c)      any member of the general public.  
The persons referred to in point (c) shall be permitted to access at least the name, the month and year of birth and the country of residence and nationality of the beneficial owner as well as the nature and extent of the beneficial interest held.  
Member States may, under conditions to be determined in national law, provide for access to additional information enabling the identification of the beneficial owner. That additional information shall include at least the date of birth or contact details in accordance with data protection rules.  
5a.            Member States may choose to make the information held in their national registers referred to in paragraph 3 available on the condition of online registration and the payment of a fee, which shall not exceed the administrative costs of making the information available, including costs of maintenance and developments of the register.  
…  
9.      In exceptional circumstances to be laid down in national law, where the access referred to in points (b) and (c) of the first subparagraph of paragraph 5 would expose the beneficial owner to disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable, Member States may provide for an exemption from such access to all or part of the information on the beneficial ownership on a case-by-case basis. Member States shall ensure that these exemptions are granted upon a detailed evaluation of the exceptional nature of the circumstances. Rights to an administrative review of the exemption decision and to an effective judicial remedy shall be guaranteed. A Member State that has granted exemptions shall publish annual statistical data on the number of exemptions granted and reasons stated and report the data to the Commission.  
…’  
9        Article 41(1) of Directive 2015/849 as amended provides:  
‘The processing of personal data under this Directive is subject to Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], as transposed into national law. …’  
   
The GDPR  
10      Article 5 of the GDPR, entitled ‘Principles relating to processing of personal data’, provides in paragraph 1:  
‘Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; … (“purpose limitation”);  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
…  
(f)      processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).’  
11      Article 25 of that regulation, entitled ‘Data protection by design and by default’, provides in paragraph 2:   
‘The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.’  
12      Article 44 of that regulation, entitled ‘General principle for transfers’, states:  
‘Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.’  
13      Article 49 of the GDPR, entitled ‘Derogations for specific situations’, provides:  
‘1.      In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:  
…  
(g)      the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.  
…’  
14      Article 94 of that regulation provides:  
‘1.      Directive 95/46/EC is repealed with effect from 25 May 2018.  
2.      References to the repealed Directive shall be construed as references to this Regulation. …’  
   
Luxembourg law  
15      Article 2 of the loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs (  
Mémorial  
 A 2019, No 15) (Law of 13 January 2019 establishing a Register of Beneficial Ownership; ‘the Law of 13 January 2019’) is worded as follows:  
‘A register known as the “Register of beneficial ownership”, abbreviated “RBO”, shall be established under the authority of the Minister responsible for Justice, the purpose of which is to retain and make available information on the beneficial ownership of registered entities.’  
16      Article 3(1) of that law provides:  
‘The following information on the beneficial owners of registered entities must be entered and retained in the Register of Beneficial Ownership:  
1°      surname;  
2°      forename(s);  
3°      nationality (or nationalities);  
4°      day of birth;  
5°      month of birth;  
6°      year of birth;  
7°      place of birth;  
8°      country of residence;  
9°      complete private or professional address …  
…  
10°      for persons registered in the National Register of Natural Persons, the identification number …;  
11°      for non-residents who are not registered in the National Register of Natural Persons, a foreign identification number;  
12°      the nature of the beneficial interests held;  
13°      the extent of the beneficial interests held.’  
17      Article 11(1) of the Law of 13 January 2019 provides:  
‘In the performance of their duties, the national authorities shall have access to the information referred to in Article 3.’  
18      Article 12 of that law provides:  
‘Access to the information referred to in Article 3(1), (1) to (8), (12) and (13) shall be open to any person.’  
19      Article 15(1) and (2) of the Law of 13 January 2019 provides:  
‘A registered entity or a beneficial owner may request, on a case-by-case basis and in the following exceptional circumstances, by way of a duly reasoned application addressed to the Administrator, that access to the information listed in Article 3 be restricted to national authorities, credit institutions, financial institutions, bailiffs and notaries acting in their capacity as public officers, where access to that information would expose the beneficial owner to disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable.  
The Administrator shall provisionally restrict access to the information listed in Article 3 to national authorities upon receipt of the application and until notification of its decision and, in the event that the application is refused, for an additional period of 15 days. Where an appeal is lodged against a refusal decision, the restriction of access to the information shall be maintained until such time as the refusal decision is no longer amenable to appeal.’  
   
The disputes in the main proceedings and the questions referred for a preliminary ruling  
   
Case   
C  
-  
37  
/20  
20      YO, a real estate company, lodged an application with LBR, pursuant to Article 15 of the Law of 13 January 2019, requesting that access to the information concerning WM, its beneficial owner, contained in the RBO, be restricted solely to the entities mentioned in that provision, on the ground that the general public’s access to that information would seriously, actually and immediately expose WM and his family to a disproportionate risk and risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation. That application was rejected by decision of 20 November 2019.  
21      On 5 December 2019, WM brought an action before the tribunal d’arrondissement de Luxembourg (Luxembourg District Court, Luxembourg), the referring court, maintaining that his position as executive officer and beneficial owner of YO and of a number of commercial companies requires him frequently to travel to countries whose political regime is unstable and where there is a high level of crime, which creates a significant risk of his being kidnapped, abducted, subjected to violence or even killed.  
22      LBR disputes that argument and contends that WM’s situation does not meet the requirements of Article 15 of the Law of 13 January 2019, since WM cannot rely either on ‘exceptional circumstances’ or on any of the risks referred to in that article.  
23      In that regard, the referring court raises the question of the interpretation to be given to the concepts of ‘exceptional circumstances’, ‘risk’ and ‘disproportionate’ risk within the meaning of Article 30(9) of Directive 2015/849 as amended.  
24      In those circumstances, the tribunal d’arrondissement de Luxembourg (Luxembourg District Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      The concept of “exceptional circumstances”  
(a)      Is Article 30(9) of [Directive 2015/849 as amended], in so far as it makes the restriction of access to information concerning beneficial owners conditional upon “exceptional circumstances to be laid down in national law”, to be interpreted as allowing national law to define the concept of “exceptional circumstances” simply as being equivalent to “disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation”, concepts which already constitute a condition for applying the restriction of access in accordance with the wording of Article 30(9) of [Directive 2015/849 as amended]?  
(b)      In the event that Question 1(a) is answered in the negative, and in the situation where the transposing national law has not defined the concept of “exceptional circumstances” other than by a reference to the ineffective concepts of “disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation”, is Article 30(9) [of Directive 2015/849 as amended] to be interpreted as allowing a national court to disregard the condition of “exceptional circumstances”, or must it make good the national legislature’s omission by using its own authority to determine the scope of the concept of “exceptional circumstances”? In the latter case, since, according to the wording of Article 30(9) [of Directive 2015/849 as amended], that is a condition whose content is to be determined by national law, is it possible for the Court … to give guidance to the national court for that purpose? In the event that that last question is answered in the affirmative, what guidelines should the national court follow in determining the content of the concept of “exceptional circumstances”?  
(2)      The concept of “risk”  
(a)      Is Article 30(9) of [Directive 2015/849 as amended], in so far as it makes the restriction of access to information concerning beneficial owners conditional upon “disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation”, to be interpreted as referring to a group of eight cases, the first of which corresponds to a general risk subject to the disproportionality requirement, while the other seven correspond to specific risks not subject to the disproportionality requirement, or as referring to a group of seven cases, each of which corresponds to a specific risk subject to the disproportionality requirement?  
(b)      Is Article 30(9) of [Directive 2015/849 as amended], in so far as it makes the restriction of access to information concerning beneficial owners conditional upon a “risk”, to be interpreted as confining the assessment of the existence and extent of that risk solely to the relationships which the beneficial owner has with the legal entity with regard to which he or she specifically seeks to have access to information concerning his or her status as beneficial owner restricted or as also requiring account to be taken of the relationships which the beneficial owner concerned has with other legal entities? If account must be taken of relationships with other legal entities, must account be taken only of the status of beneficial owner in relation to other legal entities or must account also be taken of any relationship whatsoever with other legal entities? If account must be taken of any relationship whatsoever with other legal entities, is the assessment of the existence and extent of the risk affected by the nature of that relationship?  
(c)      Is Article 30(9) of [Directive 2015/849 as amended], in so far as it makes the restriction of access to information concerning beneficial owners conditional upon a “risk”, to be interpreted as meaning that the protection resulting from restriction of access is not afforded where that information, or any other information provided by the beneficial owner to demonstrate the existence and extent of the “risk” faced, is easily available to third parties through other information channels?  
(3)      The concept of “disproportionate risk”  
What competing interests must be taken into consideration in the context of applying Article 30(9) of [Directive 2015/849 as amended], in so far as it makes the restriction of access to information concerning a beneficial owner conditional upon a “disproportionate” risk?’  
   
Case   
C  
-  
601  
/20  
25      Sovim lodged an application with LBR, pursuant to Article 15 of the Law of 13 January 2019, requesting that access to the information concerning its beneficial owner, contained in the RBO, be restricted solely to the entities mentioned in that provision. That application was rejected by decision of 6 February 2020.  
26      On 24 February 2020, Sovim brought an action before the referring court.  
27      Principally, Sovim seeks a declaration that Article 12 of the Law of 13 January 2019, pursuant to which access to certain information contained in the RBO is open to ‘any person’, and/or Article 15 of that law are inapplicable and an order for the information provided by Sovim pursuant to Article 3 of that law not to be made publicly accessible.  
28      In that regard, Sovim submits, in the first place, that granting public access to the identity and personal data of its beneficial owner would infringe the right to respect for private and family life and the right to the protection of personal data, enshrined respectively in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
29      In that company’s view, the aims of Directive 2015/849 as amended, on the basis of which the Law of 13 January 2019 was introduced into Luxembourg law, are to identify the beneficial owners of companies used for the purposes of money laundering or terrorist financing, as well as to ensure certainty in commercial relationships and market confidence. However, it has not been shown how granting the public entirely unrestricted access to the data held in the RBO enables those aims to be attained.  
30      In the second place, Sovim submits that public access to personal data contained in the RBO constitutes an infringement of several provisions of the GDPR, in particular a number of fundamental principles set out in Article 5(1) thereof.  
31      In the alternative, Sovim claims that the referring court should hold that there is a disproportionate risk in the present case, within the meaning of Article 15(1) of the Law of 13 January 2019, and accordingly make an order requiring LBR to restrict access to the information referred to in Article 3 of that law.  
32      In that regard, the referring court observes that Article 15(1) of the Law of 13 January 2019 provides that LBR must carry out a case-by-case analysis of whether there are exceptional circumstances justifying a restriction of access to the RBO. While, in the context of that law, several questions have already been referred to the Court in Case C-37/20, concerning the interpretation of the concepts of ‘exceptional circumstances’, ‘risk’ and ‘disproportionate’ risk, the present proceedings in Case C-601/20 also raise other issues, in particular that of whether the general public’s access to some of the data in the RBO is compatible with the Charter and also with the GDPR.  
33      In those circumstances, the tribunal d’arrondissement de Luxembourg (Luxembourg District Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 1(15)(c) of [Directive 2018/843], amending the first subparagraph of Article 30(5) of [Directive 2015/849], in so far as it requires Member States to make information on beneficial owners accessible to the general public in all cases, with no requirement for a legitimate interest to be shown, a valid provision:  
–        in the light of the right to respect for private and family life guaranteed in Article 7 of the [Charter], interpreted in accordance with Article 8 of the European Convention on Human Rights, having regard to the objectives stated, inter alia, in recitals 30 and 31 of Directive 2018/843 relating, in particular, to efforts to combat money laundering and terrorist financing; and  
–        in the light of the right to the protection of personal data guaranteed by Article 8 of the Charter, in so far as it is intended, inter alia, to guarantee that personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject, that the purposes for which such data are collected and processed are limited, and that the data are minimised?  
(2)      (a)      Is Article 1(15)(g) of Directive 2018/843 to be interpreted as meaning that the exceptional circumstances to which it refers – in which Member States may provide for exemptions from access to all or part of the information on beneficial owners, where access on the part of the general public would expose the beneficial owner to disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation – may be found only where it is demonstrated that there is a disproportionate risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation which is exceptional, which is actually borne by the beneficial owner as an individual, and which is significant, real and present?  
(b)      If that question is answered in the affirmative, is Article 1(15)(g) of Directive 2018/843, thus interpreted, a valid provision in the light of the right to respect for private and family life guaranteed by Article 7 of the Charter and the right to the protection of personal data guaranteed by Article 8 of the Charter?  
(3)      (a)      Is Article 5(1)(a) of [the GDPR], which requires data to be processed lawfully, fairly and in a transparent manner in relation to the data subject, to be interpreted as not precluding:  
–        that the personal data of a beneficial owner, recorded in a register of beneficial ownership, established in accordance with Article 30 of Directive 2015/849, as amended by Article 1(15) of Directive 2018/843, is accessible to the general public, with no monitoring of access and no requirement for any member of the public to provide justification, and without the data subject (the beneficial owner) having any way of discovering who has accessed his or her personal data; or  
–        that the data controller responsible for such a register of beneficial ownership provides access to the personal data of beneficial owners to an unlimited and indeterminable number of persons?  
(b)      Is Article 5(1)(b) of the GDPR, which requires the purposes of data processing to be limited, to be interpreted as not precluding that the personal data of a beneficial owner, recorded in a register of beneficial ownership established in accordance with Article 30 of [Directive 2015/849 as amended], is accessible to the general public, in circumstances where the data controller cannot guarantee that those data will be used only for the purpose for which they were collected, which is, in essence, the combating of money laundering and terrorist financing – a purpose in relation to which the general public is not the body responsible for compliance?  
(c)      Is Article 5(1)(c) of the GDPR, which requires data to be minimised, to be interpreted as not precluding the general public from having access, through a register of beneficial ownership established in accordance with Article 30 of [Directive 2015/849 as amended], to data indicating, in addition to the beneficial owner’s name, month and year of birth, nationality and country of residence, as well as the nature and extent of his or her beneficial interests, also his or her date and place of birth?  
(d)      Does Article 5(1)(f) of the GDPR, which requires data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and thus guarantees the integrity and confidentiality of such data, not preclude the provision of access to the personal data of beneficial owners held in a register of beneficial ownership, established in accordance with Article 30 of [Directive 2015/849 as amended], on an unlimited and unconditional basis and with no undertaking to preserve the confidentiality of those data?  
(e)      Is Article 25(2) of the GDPR, which guarantees data protection by default, providing in particular that, by default, personal data must not be made accessible without the individual’s intervention to an indefinite number of natural persons, to be interpreted as not precluding:  
–        that a register of beneficial ownership, established in accordance with Article 30 of [Directive 2015/849 as amended], does not require members of the general public consulting the personal data of a beneficial owner on its website to create an account; or  
–        that no information concerning the consultation of the personal data of a beneficial owner contained in such a register is disclosed to that beneficial owner; or  
–        that no restriction on the extent and accessibility of the personal data at issue is applicable in the light of the purpose of their processing?  
(f)      Are Articles 44 to 50 of the GDPR, under which the transfer of personal data to a third country is subject to strict conditions, to be interpreted as not precluding that the personal data of a beneficial owner, contained in a register of beneficial ownership established in accordance with Article 30 of [Directive 2015/849 as amended], are accessible in any circumstances to any member of the general public, with no requirement to demonstrate a legitimate interest and no limitations as to the location of that public?’  
   
Consideration of the questions referred  
   
The first question referred in Case   
C  
-  
601  
/20  
34      By the first question referred in Case C-601/20, the referring court raises the issue, in essence, of the validity, in the light of Articles 7 and 8 of the Charter, of Article 1(15)(c) of Directive 2018/843, in so far as that provision amended point (c) of the first subparagraph of Article 30(5) of Directive 2015/849 in such a way that that point (c), as thus amended, provides that Member States must ensure that information on the beneficial ownership of companies and of other legal entities incorporated within their territory is accessible in all cases to any member of the general public.  
   
The interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, resulting from the general public’s access to information on beneficial ownership  
35      Article 7 of the Charter guarantees everyone the right to respect for his or her private and family life, home and communications, while Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her.  
36      As is apparent from Article 30(1) and (3) of Directive 2015/849 as amended, Member States must ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership and that that information is held in a central register in each Member State. Under Article 3(6) of that directive, beneficial owners mean any natural person (or persons) who ultimately owns or controls the customer and/or the natural person (or persons) on whose behalf a transaction or activity is being conducted.  
37      Point (c) of the first subparagraph of Article 30(5) of Directive 2015/849 as amended requires Member States to ensure that the information on beneficial ownership is accessible in all cases to ‘any member of the general public’, while the second subparagraph of Article 30(5) states that the persons referred to in that point (c) must be permitted ‘to access at least the name, the month and year of birth and the country of residence and nationality of the beneficial owner as well as the nature and extent of the beneficial interest held’. Article 30(5) adds, in its third subparagraph, that ‘Member States may, under conditions to be determined in national law, provide for access to additional information enabling the identification of the beneficial owner’, which ‘shall include at least the date of birth or contact details in accordance with data protection rules.’  
38      In that regard, it should be noted that since the data referred to in Article 30(5) include information on identified individuals, namely the beneficial owners of corporate and other legal entities incorporated within the Member States’ territory, the access of any member of the general public to those data affects the fundamental right to respect for private life, guaranteed in Article 7 of the Charter (see, by analogy, judgment of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraph 94 and the case-law cited), it being of no relevance in that respect that the data concerned may relate to activities of a professional nature (see, by analogy, judgment of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 59). In addition, making available those data to the general public in that manner constitutes the processing of personal data falling under Article 8 of the Charter (see, by analogy, judgment of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 52 and 60).  
39      It should also be noted that, as is apparent from the Court’s settled case-law, making personal data available to third parties constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. In that connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (judgment of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraph 96 and the case-law cited).  
40      Consequently, the general public’s access to information on beneficial ownership, provided for in Article 30(5) of Directive 2015/849 as amended, constitutes an interference with the rights guaranteed in Articles 7 and 8 of the Charter.  
41      As regards the seriousness of that interference, it is important to note that, in so far as the information made available to the general public relates to the identity of the beneficial owner as well as to the nature and extent of the beneficial interest held in corporate or other legal entities, that information is capable of enabling a profile to be drawn up concerning certain personal identifying data more or less extensive in nature depending on the configuration of national law, the state of the person’s wealth and the economic sectors, countries and specific undertakings in which he or she has invested.  
42      In addition, it is inherent in making that information available to the general public in such a manner that it is then accessible to a potentially unlimited number of persons, with the result that such processing of personal data is liable to enable that information to be freely accessed also by persons who, for reasons unrelated to the objective pursued by that measure, seek to find out about, inter alia, the material and financial situation of a beneficial owner (see, by analogy, judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraphs 102 and 103). That possibility is all the easier when, as is the case in Luxembourg, the data in question can be consulted on the internet.  
43      Furthermore, the potential consequences for the data subjects resulting from possible abuse of their personal data are exacerbated by the fact that, once those data have been made available to the general public, they can not only be freely consulted, but also retained and disseminated and that, in the event of such successive processing, it becomes increasingly difficult, or even illusory, for those data subjects to defend themselves effectively against abuse.  
44      Accordingly, the general public’s access to information on beneficial ownership, provided for in point (c) of the first subparagraph of Article 30(5) of Directive 2015/849 as amended, constitutes a serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter (see, by analogy, judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 105).  
   
The justification for the interference resulting from the general public’s access to information on beneficial ownership  
45      The fundamental rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (judgment of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraph 112 and the case-law cited).  
46      Under the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. According to the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made on those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. In that connection, Article 8(2) of the Charter states that personal data must, inter alia, be processed ‘for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.  
–         
Observance of the principle of legality  
47      As regards the requirement that any limitation on the exercise of fundamental rights must be provided for by law, this implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned, bearing in mind, on the one hand, that that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances and, on the other hand, that the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter (judgment of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraph 114 and the case-law cited).  
48      In that regard, it should be noted that the limitation on the exercise of the fundamental rights guaranteed in Articles 7 and 8 of the Charter, resulting from the general public’s access to information on beneficial ownership, is provided for by an EU legislative act, namely Directive 2015/849 as amended. In addition, Article 30(1) and (5) of that directive provides, first, for access by the general public to data relating to the identification of the beneficial owners and the beneficial interest which they hold, specifying that those data must be adequate, accurate and current, and expressly listing certain of those data to which any member of the general public must be allowed access. Secondly, Article 30(9) of Directive 2015/849 as amended lays down the conditions under which Member States may provide for exemptions from such access.  
49      In those circumstances, the principle of legality must be considered to have been fulfilled.  
–         
Respect for the essence of the fundamental rights guaranteed in Articles 7 and 8 of the Charter  
50      As regards respect for the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter, it should be noted that the information expressly referred to in the second subparagraph of Article 30(5) of Directive 2015/849 as amended may be classified into two distinct categories of data: the first comprising data relating to the identity of the beneficial owner (name, month and year of birth, and nationality) and the second comprising economic data (nature and extent of the beneficial interest held).  
51      Furthermore, while the second subparagraph of Article 30(5) of Directive 2015/849 as amended does not – as is clear from the use of the expression ‘at least’ – contain an exhaustive list of the data which any member of the general public must be permitted to access, and the third subparagraph of Article 30(5) adds that Member States are entitled to provide for access to additional information, the fact remains that, in accordance with Article 30(1), only ‘adequate’ information on beneficial owners and beneficial interests held may be obtained, held and, therefore, potentially made accessible to the public, which excludes, inter alia, information which is not adequately related to the purposes of that directive.  
52      As it is, it does not appear that making available to the general public information which is so related would in any way undermine the essence of the fundamental rights guaranteed in Articles 7 and 8 of the Charter.  
53      In that context, it should also be noted that Article 41(1) of Directive 2015/849 as amended expressly provides that the processing of personal data under that directive is subject to Directive 95/46 and, therefore, to the GDPR, Article 94(2) of which states that references to Directive 95/46 are to be construed as references to the GDPR. It is, therefore, established that any collection, storage and making available of information under Directive 2015/849 as amended must fully meet the requirements arising from the GDPR.  
54      In those circumstances, the interference entailed by the general public’s access to information on beneficial ownership provided for in point (c) of the first subparagraph of Article 30(5) of Directive 2015/849 as amended does not undermine the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter.  
–         
The objective of general interest recognised by the European Union  
55      Directive 2015/849 as amended aims, in the words of Article 1(1) thereof, to prevent the use of the European Union’s financial system for the purposes of money laundering and terrorist financing. In that regard, recital 4 of Directive 2018/843 states that the pursuit of that objective cannot be effective unless the environment is hostile to criminals and that enhancing the overall transparency of the economic and financial environment of the European Union could be a powerful deterrent.  
56      As regards, more specifically, the objective of the general public’s access to information on beneficial ownership, introduced by Article 1(15)(c) of Directive 2018/843, recital 30 of that directive states that such access, first of all, ‘allows greater scrutiny of information by civil society, including by the press or civil society organisations, and contributes to preserving trust in the integrity of business transactions and of the financial system’. Next, the access in question ‘can contribute to combating the misuse of corporate and other legal entities and legal arrangements for the purposes of money laundering or terrorist financing, both by helping investigations and through reputational effects, given that anyone who could enter into transactions is aware of the identity of the beneficial owners’. Lastly, that access ‘also facilitates the timely and efficient availability of information for financial institutions as well as authorities, including authorities of third countries, involved in combating such offences’ and ‘would also help investigations on money laundering, associated predicate offences and terrorist financing’.  
57      Furthermore, recital 31 of Directive 2018/843 states that ‘the potential increase in confidence in financial markets should be regarded as a positive side effect and not the purpose of increasing transparency, which is to create an environment less likely to be used for the purposes of money laundering and terrorist financing’.  
58      It follows that, by providing for the general public’s access to information on beneficial ownership, the EU legislature seeks to prevent money laundering and terrorist financing by creating, by means of increased transparency, an environment less likely to be used for those purposes.  
59      That aim constitutes an objective of general interest that is capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter (see, to that effect, judgment of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraph 122 and the case-law cited).  
60      In so far as the Council of the European Union also refers, in that context, expressly to the principle of transparency, as follows from Articles 1 and 10 TEU and from Article 15 TFEU, it should be noted that that principle, as the Council itself states, enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system (judgment of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 68 and the case-law cited).  
61      While, in that respect, the principle of transparency is given concrete expression primarily in the requirements of institutional and procedural transparency covering activities of a public nature, including the use of public funds, such a link with public institutions is lacking where, as in the present case, the measure at issue is intended to make available to the general public data concerning the identity of private beneficial owners and the nature and extent of their beneficial interests held in companies or other legal entities.  
62      Accordingly, the principle of transparency, as it results from Articles 1 and 10 TEU and from Article 15 TFEU, cannot be considered, as such, an objective of general interest capable of justifying the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, which results from the general public’s access to information on beneficial ownership.  
–         
Whether the interference at issue is appropriate, necessary and proportionate  
63      According to settled case-law, the proportionality of the measures which result in interference with the rights guaranteed in Articles 7 and 8 of the Charter requires compliance not only with the requirements of appropriateness and of necessity but also with that of the proportionate nature of those measures in relation to the objective pursued (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 93).  
64      More specifically, derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary, it being understood that where there is a choice between several measures appropriate to meeting the legitimate objectives pursued, recourse must be had to the least onerous. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue, in order to ensure that the disadvantages caused by that measure are not disproportionate to the aims pursued. Thus, the question whether a limitation on the rights guaranteed in Articles 7 and 8 of the Charter may be justified must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness (see, to that effect, judgments of 26 April 2022,   
Poland  
 v   
Parliament and Council  
, C-401/19, EU:C:2022:297, paragraph 65, and of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraphs 115 and 116 and the case-law cited).  
65      Furthermore, in order to satisfy the proportionality requirement, the legislation in question entailing the interference must also lay down clear and precise rules governing the scope and application of the measures provided for and imposing minimum safeguards, so that the data subjects have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are made accessible to the general public, and thus to a potentially unlimited number of persons, and are liable to reveal sensitive data on the data subjects (see, to that effect, judgment of 21 June 2022,   
Ligue des droits humains  
, C-817/19, EU:C:2022:491, paragraph 117 and the case-law cited).  
66      In accordance with that case-law, it is necessary to ascertain, first, whether the general public’s access to information on beneficial ownership is appropriate for attaining the objective of general interest pursued, secondly, whether the interference with the rights guaranteed in Articles 7 and 8 of the Charter which results from such access is limited to what is strictly necessary, in the sense that the objective could not reasonably be achieved in an equally effective manner by other means less prejudicial to those fundamental rights of the data subjects, and, thirdly, whether that interference is not disproportionate to that objective, which implies, in particular, a balancing of the importance of the objective and the seriousness of the interference.  
67      In the first place, it must be held that the general public’s access to information on beneficial ownership is appropriate for contributing to the attainment of the objective of general interest, identified in paragraph 58 above, of seeking to prevent money laundering and terrorist financing, since the public nature of that access and the increased transparency resulting therefrom contribute to the creation of an environment less likely to be used for such purposes.  
68      In the second place, in order to demonstrate that the interference resulting from the general public’s access to information on beneficial ownership is strictly necessary, the Council and the Commission refer to the impact assessment accompanying the Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC (COM(2016) 450 final), which gave rise to Directive 2018/843. According to those institutions, whereas point (c) of the first subparagraph of Article 30(5) of Directive 2015/849, in the version prior to its amendment by Directive 2018/843, made access by any person to information on beneficial ownership conditional upon that person being able to demonstrate a ‘legitimate interest’, that impact assessment found that the lack of a uniform definition of that concept of ‘legitimate interest’ had given rise to practical difficulties, with the result that it was considered that the appropriate solution was to remove that condition.  
69      Furthermore, in their written observations, the Parliament, the Council and the Commission state, referring in particular to recital 30 of Directive 2018/843, that the general public’s access to information on beneficial ownership, as provided for by Directive 2015/849 as amended, has a deterrent effect, enables greater scrutiny and facilitates the conduct of investigations, including those carried out by the authorities of third countries, and that those consequences could not be achieved in any other way.  
70      At the hearing, the Commission was asked to indicate whether it had considered proposing a uniform definition of ‘legitimate interest’, in order to offset the risk that the obligation for any person or organisation to demonstrate such an interest, as initially provided for by Directive 2015/849, might lead to excessive limitations on access to information on beneficial ownership, owing to differences in the definition of ‘legitimate interest’ in the Member States.  
71      In response to that question, the Commission observed that the criterion of ‘legitimate interest’ was a concept which did not lend itself easily to a legal definition and that, while it had considered the possibility of proposing a uniform definition of that criterion, it had ultimately decided not to do so on the ground that the criterion, even if defined, remained difficult to apply and that its application could give rise to arbitrary decisions.  
72      In that regard, it must be noted that the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which the public may access information on beneficial ownership is no reason for the EU legislature to provide for the general public to access that information (see, by analogy, judgment of 5 April 2022,  
 Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 84).  
73      Moreover, nor can the effects relied on and the reference made, in that context, to the explanations set out in recital 30 of Directive 2018/843 establish that the interference at issue is strictly necessary.  
74      To the extent that that recital states that the general public’s access to beneficial ownership information allows greater scrutiny of information by civil society, and that express reference is made in that regard to the press and to civil society organisations, it should be found that both the press and civil society organisations that are connected with the prevention and combating of money laundering and terrorist financing have a legitimate interest in accessing information on beneficial ownership. The same is true of the persons, also mentioned in that recital, who wish to know the identity of the beneficial owners of a company or other legal entity because they are likely to enter into transactions with them, or of the financial institutions and authorities involved in combating offences of money laundering or terrorist financing, in so far as those entities do not already have access to the information in question on the basis of points (a) and (b) of the first subparagraph of Article 30(5) of Directive 2015/849 as amended.  
75      Moreover, although it is stated in recital 30 of Directive 2018/843 that the general public’s access to information on beneficial ownership ‘can contribute’ to combating the misuse of corporate and other legal entities and that it ‘would also help’ criminal investigations, it must be found that such considerations are also not such as to demonstrate that that measure is strictly necessary to prevent money laundering and terrorist financing.  
76      In the light of the foregoing, it cannot be considered that the interference with the rights guaranteed in Articles 7 and 8 of the Charter, which results from the general public’s access to information on beneficial ownership, is limited to what is strictly necessary.  
77      In the third place, as regards the factors put forward to establish that the interference at issue is proportionate, in that, in particular, the general public’s access to information on beneficial ownership, provided for in Article 30(5) of Directive 2015/849 as amended, is based on a proper balance between, on the one hand, the objective of general interest pursued and, on the other, the fundamental rights at issue, and that there are sufficient safeguards against the risks of abuse, the following points must be made.  
78      First of all, the Commission contends that, as is apparent from recital 34 of Directive 2018/843, the EU legislature took care to specify that the set of data made available to the public must be limited, clearly and exhaustively defined, and must be of a general nature, so as to minimise the potential prejudice to beneficial owners. It is in that context that, on the basis of Article 30(5) of Directive 2015/849 as amended, only data strictly necessary to identify the beneficial owners and the nature and extent of their interests would be accessible to the public.  
79      Next, the Parliament, the Council and the Commission state that the principle that the general public should have access to information on beneficial ownership may be derogated from, since Article 30(9) of Directive 2015/849 as amended provides that in ‘exceptional circumstances’, ‘Member States may provide for an exemption from such access to all or part of the information on the beneficial ownership on a case-by-case basis’ where the general public’s access to that information ‘would expose the beneficial owner to disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable’.  
80      Lastly, both the Parliament and the Commission observe that, as is apparent from Article 30(5a) of Directive 2015/849 as amended, read in conjunction with recital 36 of Directive 2018/843, Member States may make the information on beneficial ownership available on condition of online registration in order to identify the person requesting that information. In addition, in accordance with recital 38 of Directive 2018/843, in order to prevent the abuse of the information on beneficial ownership, Member States might make information relating to the requesting person along with the legal basis for their request available to the beneficial owner.  
81      In that regard, it should be noted that, as recalled in paragraph 51 above, the second subparagraph of Article 30(5) of Directive 2015/849 as amended provides that any member of the general public is to be permitted to access ‘at least’ the data referred to in that provision, and the third subparagraph of Article 30(5) adds that Member States may provide for access to ‘additional information enabling the identification of the beneficial owner’, which includes ‘at least’ the date of birth or the contact details of the beneficial owner concerned.  
82      However, it is apparent from the use of the expression ‘at least’ that those provisions allow for data to be made available to the public which are not sufficiently defined and identifiable. Consequently, the substantive rules governing interference with the rights guaranteed in Articles 7 and 8 of the Charter do not meet the requirement of clarity and precision recalled in paragraph 65 above (see, by analogy, Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, paragraph 160).  
83      Furthermore, as regards the balancing of the seriousness of that interference, identified in paragraphs 41 to 44 above, against the importance of the objective of general interest of preventing money laundering and terrorist financing, it must be held that although in view of its importance that objective is, as found in paragraph 59 above, capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter, the fact remains that, first, combating money laundering and terrorist financing is as a priority a matter for the public authorities and for entities such as credit or financial institutions which, by reason of their activities, are subject to specific obligations in that regard.  
84      Indeed, it is for that reason that points (a) and (b) of the first subparagraph of Article 30(5) of Directive 2015/849 as amended provide that information on beneficial ownership must be accessible, in all cases, to competent authorities and Financial Intelligence Units, without any restriction, as well as to obliged entities, within the framework of customer due diligence.  
85      Secondly, in comparison with a regime such as that laid down in the version of Article 30(5) of Directive 2015/849 prior to the entry into force of Directive 2018/843 – which provided, in addition to access by the competent authorities and certain entities, for access by any person or organisation capable of demonstrating a legitimate interest – the regime introduced by Directive 2018/843, providing for the general public’s access to information on beneficial ownership, amounts to a considerably more serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, without that increased interference being capable of being offset by any benefits which might result from the latter regime as compared against the former regime, in terms of combating money laundering and terrorist financing (see, by analogy, judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 112).  
86      In those circumstances, the optional provisions of Article 30(5a) and (9) of Directive 2015/849 as amended, which allow Member States to make information on beneficial ownership available on condition of online registration and to provide, in exceptional circumstances, for an exemption from access to that information by the general public, respectively, are not, in themselves, capable of demonstrating either a proper balance between the objective of general interest pursued and the fundamental rights enshrined in Articles 7 and 8 of the Charter, or the existence of sufficient safeguards enabling data subjects to protect their personal data effectively against the risks of abuse.  
87      Moreover, the Commission’s reference to the judgment of 9 March 2017,   
Manni  
 (C-398/15, EU:C:2017:197), – concerning compulsory disclosure by companies, including of their representatives in legal proceedings, provided for in First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community (OJ 1968 L 65, p. 8), as amended by Directive 2003/58/EC of the European Parliament and of the Council of 15 July 2003 (OJ 2003 L 221, p. 3) – is irrelevant in that context. Indeed, the compulsory disclosure provided for by that directive, on the one hand, and the general public’s access to information on beneficial ownership, provided for by Directive 2015/849 as amended, on the other, differ both in their respective purposes and in their scope in terms of the personal data covered.  
88      In the light of all the foregoing considerations, the answer to the first question referred in Case C-601/20 is that Article 1(15)(c) of Directive 2018/843 is invalid in so far as it amended point (c) of the first subparagraph of Article 30(5) of Directive 2015/849 in such a way that point (c), as thus amended, provides that Member States must ensure that information on the beneficial ownership of companies and of other legal entities incorporated within their territory is accessible in all cases to any member of the general public.  
   
The second and third questions referred in Case   
C  
-  
601  
/20 and the questions referred in Case   
C  
-  
37  
/20  
89      The second question referred in Case C-601/20 and the questions referred in Case C-37/20 are based on the premiss that Article 30(5) of Directive 2015/849 as amended is valid, in so far as it provides for public access to information on beneficial ownership.  
90      However, in view of the answer to the first question referred in Case C-601/20, there is no need to examine those questions.  
91      Furthermore, in the light of that same answer, there is also no need to adjudicate on the third question referred in Case C-601/20.  
   
Costs  
92      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
Article 1(15)(c) of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, is invalid in so far as it amended point (c) of the first subparagraph of Article 30(5) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, in such a way that point (c) of the first subparagraph of Article 30(5), as thus amended, provides that Member States must ensure that information on the beneficial ownership of companies and of other legal entities incorporated within their territory is accessible in all cases to any member of the general public.

ID: a9cd6ec2-819b-405c-8e2a-ba1aa5ff9635

Judgment of 9 Nov 2010, C-92/09 (  
Volker und Markus Schecke and Eifert  
)  
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Obligation to notify the supervisory authority   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Records of processing activities   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Data protection officer   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Prior consultation   
   
JUDGMENT OF THE COURT (Grand Chamber)  
9 November 2010 (\*)  
(Protection of natural persons with regard to the processing of personal data – Publication of information on beneficiaries of agricultural aid – Validity of the provisions of European Union law providing for that publication and laying down detailed rules for such publication – Charter of Fundamental Rights of the European Union – Articles 7 and 8 – Directive 95/46/EC – Interpretation of Articles 18 and 20)  
In Joined Cases C-92/09 and C-93/09,  
REFERENCES for preliminary rulings under Article 234 EC from the Verwaltungsgericht Wiesbaden (Germany), made by decisions of 27 February 2009, received at the Court on 6 March 2009, in the proceedings  
Volker und Markus Schecke GbR  
 (C-92/09),  
Hartmut Eifert   
(C-93/09)  
v  
Land Hessen,  
joined party:  
Bundesanstalt für Landwirtschaft und Ernährung,  
THE COURT (Grand Chamber),  
composed of V. Skouris, President, A. Tizzano, J.N. Cunha Rodrigues, K. Lenaerts (Rapporteur), J.-C. Bonichot, K. Schiemann, A. Arabadjiev and J.-J. Kasel, Presidents of Chambers, E. Juhász, C. Toader and M. Safjan, Judges,  
Advocate General: E. Sharpston,  
Registrar: B. Fülöp, Administrator,  
having regard to the written procedure and further to the hearing on 2 February 2010,  
after considering the observations submitted on behalf of:  
–        Volker und Markus Schecke GbR, by R. Seimetz and P. Breyer, Rechtsanwälte, and by Mr Schecke,  
–        Mr Eifert, by R. Seimetz and P. Breyer, Rechtsanwälte,  
–        Land Hessen, by H.-G. Kamann, Rechtsanwalt,  
–        the Greek Government, by V. Kontolaimos, I. Chalkias, K. Marinou and V. Karra, acting as Agents,  
–        the Netherlands Government, by C. Wissels and Y. de Vries, acting as Agents,  
–        the Swedish Government, by A. Falk and C. Meyer-Seitz, acting as Agents,  
–        the Council of the European Union, by E. Sitbon and Z. Kupčová, acting as Agents,  
–        the European Commission, by B. Smulders, F. Erlbacher and P. Costa de Oliveira, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 17 June 2010,  
gives the following  
Judgment  
1        These references for preliminary rulings concern the validity, first, of Articles 42(8b) and 44a of Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy (OJ 2005 L 209, p. 1), as amended by Council Regulation (EC) No 1437/2007 of 26 November 2007 (OJ 2007 L 322, p. 1) (‘Regulation No 1290/2005’), and, second, of Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Regulation No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) (OJ 2008 L 76, p. 28) and Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54). Should the Court find that the European Union legislation referred to above is not invalid, the references for preliminary rulings also concern the interpretation of Article 7, the second indent of Article 18(2) and Article 20 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        Those questions have been raised in the course of proceedings between Volker und Markus Schecke GbR and Mr Eifert (‘the applicants in the main proceedings’) and Land Hessen (the   
Land  
 of Hesse) concerning the publication on the internet site of the Bundesanstalt für Landwirtschaft und Ernährung (Federal Office for Agriculture and Food; ‘the Bundesanstalt’) of personal data relating to them as recipients of funds from the EAGF or the EAFRD.  
I –    
Legal context  
A –    
European Convention for the Protection of Human Rights and Fundamental Freedoms  
3        Under the heading ‘Right to respect for private and family life’, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950, (‘the Convention’) provides:  
‘1.      Everyone has the right to respect for his private and family life, his home and his correspondence.  
2.      There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.’  
B –    
European Union law  
1.     Directive 95/46  
4        In accordance with Article 1(1) of Directive 95/46, the aim of the directive is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Under Article 2(a) of the directive, ‘personal data’ means ‘any information relating to an identified or identifiable natural person’.  
5        Under Article 7 of that directive, ‘Member States shall provide that personal data may be processed only if:  
(a)      the data subject has unambiguously given his consent; or  
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject; or  
…  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; …  
…’  
6        Under Article 18(1) of the directive, ‘Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation’.  
7        Under the second indent of Article 18(2) of the directive, Member States may provide for the simplification of or exemption from notification inter alia in the following case:  
‘where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:  
–        for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive;  
–        for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2),  
thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations’.  
8        Article 19(1) of Directive 95/46 provides:  
‘Member States shall specify the information to be given in the notification. It shall include at least:  
(a)      the name and address of the controller and of his representative, if any;  
(b)      the purpose or purposes of the processing;  
(c)      a description of the category or categories of data subject and of the data or categories of data relating to them;  
(d)      the recipients or categories of recipient to whom the data might be disclosed;  
(e)      proposed transfers of data to third countries;  
…’  
9        Article 20 of the directive, ‘Prior checking’, provides in paragraphs 1 and 2:  
‘1.      Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.  
2.      Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.’  
10      In accordance with the first and second subparagraphs of Article 21(2) of Directive 95/46, ‘Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority’, and ‘[t]he register shall contain at least the information listed in Article 19(1)(a) to (e)’.  
11      Under Article 28 of the directive, each Member State is to designate one or more public authorities (‘supervisory authority’) to be responsible for monitoring, acting with complete independence, the application within that State’s territory of the national provisions adopted pursuant to that directive.  
2.     Regulation (EC) No 45/2001  
12      Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1) provides in Article 27(1) and (2):  
‘1.      Processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes shall be subject to prior checking by the European Data Protection Supervisor.  
2.      The following processing operations are likely to present such risks:  
(a)      processing of data relating to health and to suspected offences, offences, criminal convictions or security measures;  
(b)      processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct;  
(c)      processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes;  
(d)      processing operations for the purpose of excluding individuals from a right, benefit or contract.’  
3.     Directive 2006/24  
13      Directive 2006/24 requires the Member States to retain for a certain time data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.  
4.     Regulation No 1290/2005  
14      Regulation No 1290/2005 sets the specific requirements and rules on the financing of expenditure falling under the common agricultural policy (‘the CAP’).  
15      Article 42 of Regulation No 1290/2005 provides that the detailed rules for the application of that regulation are to be adopted by the European Commission. Under Article 42(8b) of the regulation, the Commission is to determine inter alia:  
‘the detailed rules on the publication of information concerning beneficiaries referred to in Article 44a and on the practical aspects related to the protection of individuals with regard to the processing of their personal data in accordance with the principles laid down in Community legislation on data protection. These rules shall ensure, in particular, that the beneficiaries of funds are informed that these data may be made public and may be processed by auditing and investigating bodies for the purpose of safeguarding the financial interests of the Communities, including the time that this information shall take place’.  
16      Article 44a of Regulation No 1290/2005, ‘Publication of the beneficiaries’, states:  
‘… Member States shall ensure annual   
ex-post  
 publication of the beneficiaries of the EAGF and the EAFRD and the amounts received per beneficiary under each of these Funds.  
The publication shall contain at least:  
(a)      for the EAGF, the amount subdivided in direct payments within the meaning of Article 2(d) of Regulation (EC) No 1782/2003 and other expenditure;  
(b)      for the EAFRD, the total amount of public funding per beneficiary.’  
17      Recitals 13 and 14 in the preamble to Regulation No 1437/2007 amending Regulation No 1290/2005 read as follows:  
‘(13) In the context of the revision of Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities [OJ 2002 L 248, p. 1], the provisions on the annual   
ex-post  
 publication of beneficiaries of funds deriving from the budget were inserted into that Regulation in order to implement the European Transparency Initiative. Sector-specific Regulations are to provide the means for such a publication. Both the EAGF and the EAFRD form part of the general budget of the European Communities and finance expenditure in a context of shared management between the Member States and the Community. Rules should therefore be laid down for the publication of information on the beneficiaries of these Funds. To that end, Member States should ensure annual   
ex-post  
 publication of the beneficiaries and the amounts received per beneficiary under each of these Funds.  
(14)      Making this information accessible to the public enhances transparency regarding the use of Community funds in the [CAP] and improves the sound financial management of these funds, in particular by reinforcing public control of the money used. Given the overriding weight of the objectives pursued, it is justified with regard to the principle of proportionality and the requirement of the protection of personal data to provide for the general publication of the relevant information as it does not go beyond what is necessary in a democratic society and for the prevention of irregularities. Taking into account the opinion of the European Data Protection Supervisor of 10 April 2007 [OJ 2007 C 134, p. 1], it is appropriate to make provision for the beneficiaries of funds to be informed that those data may be made public and that they may be processed by auditing and investigating bodies.’  
5.     Regulation No 259/2008  
18      On the basis of Article 42(8b) of Regulation No 1290/2005, the Commission adopted Regulation No 259/2008.  
19      Recital 6 in the preamble to Regulation No 259/2008 reads as follows:  
‘(6)      Making … information [concerning beneficiaries of funds from the EAGF and EAFRD] accessible to the public enhances transparency regarding the use of Community funds in the [CAP] and improves the sound financial management of these funds, in particular by reinforcing public control of the money used. Given the overriding weight of the objectives pursued, it is justified with regard to the principle of proportionality and the requirement of the protection of personal data to provide for the general publication of the relevant information as it does not go beyond what is necessary in a democratic society and for the prevention of irregularities.’  
20      Recital 7 in the preamble states that ‘[t]o comply with the data protection requirements beneficiaries of the Funds should be informed of the publication of their data before the publication takes place’.  
21      Article 1(1) of Regulation No 259/2008 specifies the content of the publication referred to in Article 44a of Regulation No 1290/2005 and provides that it is to include the following information:  
‘(a)      the first name and the surname where the beneficiaries are natural persons;  
(b)      the full legal name as registered where the beneficiaries are legal persons;  
(c)      the full name of the association as registered or otherwise officially recognised where the beneficiaries are associations of natural or legal persons without an own legal personality;  
(d)      the municipality where the beneficiary resides or is registered and, where available, the postal code or the part thereof identifying the municipality;  
(e)      for the … EAGF, the amount of direct payments within the meaning of Article 2(d) of Regulation (EC) No 1782/2003 received by each beneficiary in the financial year concerned;  
(f)      for the EAGF, the amount of payments other than those referred to in point (e) received by each beneficiary in the financial year concerned;  
(g)      for the … EAFRD, the total amount of public funding received by each beneficiary in the financial year concerned, which includes both the Community and the national contribution;  
(h)      the sum of the amounts referred to in points (e), (f) and (g) received by each beneficiary in the financial year concerned;  
(i)      the currency of these amounts.’  
22      In accordance with Article 2 of Regulation No 259/2008, ‘[the] information referred to in Article 1 shall be made available on a single website per Member State through a search tool allowing the users to search for beneficiaries by name, municipality, amounts received as referred to in (e), (f), (g) and (h) of Article 1 or a combination thereof and to extract all the corresponding information as a single set of data.’  
23      Article 3(3) of that regulation provides that ‘[t]he information shall remain available on the website for two years from the date of [its] initial publication’.  
24      Article 4 of Regulation No 259/2008 provides:  
‘1.      Member States shall inform the beneficiaries that their data will be made public in accordance with Regulation … No 1290/2005 and this Regulation and that they may be processed by auditing and investigating bodies of the Communities and the Member States for the purpose of safeguarding the Communities’ financial interests.  
2.      In case of personal data, the information referred to in paragraph 1 shall be provided in accordance with the requirements of Directive 95/46 … and the beneficiaries shall be informed of their rights as data subjects under this Directive and of the procedures applicable for exercising these rights.  
3.      The information referred to in paragraphs 1 and 2 shall be provided to the beneficiaries by including it in the application forms for receiving funds deriving from the EAGF and EAFRD, or otherwise at the time when the data are collected.  
…’  
II –    
The actions in the main proceedings and the questions referred for preliminary rulings  
25      The applicants in the main proceedings, one established and the other resident in the   
Land  
 of Hesse, are an agricultural undertaking in the legal form of a partnership (Case C-92/09) and a full-time farmer (Case C-93/09). For the financial year 2008 they made applications to the competent local authorities for funds from the EAGF or the EAFRD, which were approved by decisions of 5 December 2008 (Case C-93/09) and 31 December 2008 (Case C-92/09).  
26      In each case the application form contained the following statement:  
‘I am aware that Article 44a of Regulation … No 1290/2005 requires publication of information on the beneficiaries of [funds from] the EAGF and the EAFRD and the amounts received per beneficiary. The publication relates to all measures applied for in connection with the Common Application, which constitutes the single application for the purposes of Article 11 of Regulation (EC) No 796/2004, and is effected annually at the latest by 31 March of the following year.’  
27      The referring court explains that the Bundesanstalt’s website makes available to the public the names of beneficiaries of aid from the EAGF and the EAFRD, the place in which they are established or reside and the postcode of that place, and the annual amounts received. The site is provided with a search tool.  
28      On 26 September 2008 (Case C-92/09) and 18 December 2008 (Case C-93/09) the applicants in the main proceedings brought proceedings to prevent publication of the data relating to them. In their view, publication of the amounts received from the EAGF or the EAFRD is not justified by overriding public interests. Moreover, the rules governing the European Social Fund do not provide for beneficiaries to be identified by name. In their applications, they ask for the   
Land  
 of Hesse to be ordered to refrain from, or to be prohibited from, transmitting or publishing those data for the purposes of the general publication of information on the financial amounts granted to them from the EAGF and the EAFRD.  
29      The   
Land  
 of Hesse, which takes the view that the obligation to publish data relating to the applicants in the main proceedings follows from Regulations No 1290/2005 and No 259/2008, nevertheless undertook not to publish the amounts received by them as beneficiaries of aid from the EAGF and the EAFRD pending final decisions in the main proceedings.  
30      The referring court believes that the obligation to publish under Article 44a of Regulation No 1290/2005 constitutes an unjustified interference with the fundamental right to the protection of personal data. It considers that that provision, which pursues the aim of increasing the transparency of the use of European funds, does not improve the prevention of irregularities, since extensive control mechanisms exist at present for that purpose. On the basis of the judgment in Joined Cases C-465/00, C-138/01 and C-139/01   
Österreichischer Rundfunk and Others  
 [2003] ECR I-4989, it takes the view that, in any event, that obligation to publish is not proportionate to the aim pursued. Moreover, in its view, Article 42(8b) of Regulation No 1290/2005 gives the Commission too broad a discretion with respect to determining both the data to be published and the means of publication and is therefore incompatible with the third indent of Article 202 EC and with the fourth indent of Article 211 EC.  
31      Regardless of the validity of Articles 42(8b) and 44a of Regulation No 1290/2005, the referring court considers that Regulation No 259/2008, which prescribes that the information relating to the beneficiaries of aid from the EAGF and the EAFRD is to be published exclusively on the internet, breaches the fundamental right to the protection of personal data. It points out that the latter regulation does not limit access to the internet site concerned to ‘internet protocol’ (IP) addresses situated in the European Union. Furthermore, it is not possible to withdraw the data from the internet after the expiry of the two-year period laid down in Article 3(3) of Regulation No 259/2008. It its view, publication of the data exclusively on the internet also has a deterrent effect. First, citizens wishing to obtain information must have access to the internet. Second, those citizens run the risk of having their data stored under Directive 2006/24. It is paradoxical to strengthen the supervision of telecommunications on the one hand and to provide on the other hand that information which is intended to enable citizens to participate in public affairs is available only electronically.  
32      In case the Court should find that the provisions referred to in paragraphs 30 and 31 above are not invalid, the referring court further seeks an interpretation of a number of provisions of Directive 95/46. It considers that the publication of personal data may take place only if the measures provided for in the second indent of Article 18(2) of that directive have been taken. According to the information provided by the referring court, the German legislature, in particular that of the   
Land  
 of Hesse, has made use of the possibility under that provision. However, according to that court, the notification by the Ministry of the Environment, Rural Affairs and Consumer Protection of the   
Land  
 of Hesse to the personal data protection official was incomplete. Some information was not communicated to that official, such as the fact that the data are processed by the Bundesanstalt on behalf of the   
Land  
, in some cases with the assistance of a private third party, specific details of the deletion period and the access provider, and information on the registration of IP addresses.  
33      Moreover, according to the national court, the publication of the data relating to the beneficiaries of agricultural aid ought to have been preceded by a prior check as provided for in Article 20 of Directive 95/46. In the present case, however, a prior check was carried out, not by a central supervisory authority, but by the data protection official of the undertaking or office responsible, on the basis of incomplete notifications.  
34      Finally, the referring court is uncertain as to the lawfulness, from the point of view of Article 7(e) of Directive 95/46, of the registration of the IP addresses of users who consult the information relating to beneficiaries of aid from the EAGF and the EAFRD on the Bundesanstalt’s website.  
35      In those circumstances, the Verwaltungsgericht (Administrative Court) Wiesbaden decided to stay the proceedings and to refer the following questions, which are worded identically in Case C-92/09 and Case C-93/09, to the Court for preliminary rulings:  
‘1.      Are Article [42](8b) and Article 44a of … Regulation … No 1290/2005 …, inserted by … Regulation … No 1437/2007 …, invalid?  
2.      Is … Regulation … No 259/2008 …  
(a)      invalid, or  
(b)      valid by reason only of the fact that Directive 2006/24 … is invalid?  
If the provisions mentioned in the first and second questions are valid:  
3.      Must the second indent of Article 18(2) of Directive 95/46 … be interpreted as meaning that publication in accordance with … Regulation … No 259/2008 … may be effected only following implementation of the procedure – in lieu of notification to a supervisory authority – established by that article?  
4.      Must Article 20 of Directive 95/46 … be interpreted as meaning that publication in accordance with … Regulation … No 259/2008 … may be effected only following exercise of the prior check required by national law in that case?  
5.      If the fourth question is answered in the affirmative: Must Article 20 of Directive 95/46 … be interpreted as meaning that no effective prior check has been performed, if it was effected on the basis of a register established in accordance with the second indent of Article 18(2) of that directive which lacks an item of information prescribed?  
6.      Must Article 7 – and in this case, in particular, subparagraph (e) – of Directive 95/46 … be interpreted as precluding a practice of storing the IP addresses of the users of a homepage without their express consent?’  
36      By order of the President of the Court of 4 May 2009, Cases C-92/09 and C-93/09 were joined for the purposes of the written and oral procedure and the judgment.  
III –    
Consideration of the questions referred  
37      The decisions for reference contain questions on the validity of Regulations No 1290/2005 and No 259/2008 (Questions 1 and 2) and questions on the interpretation of Directive 95/46 (Questions 3 to 6). Before examining the substance of the case, the admissibility of the second part of Question 2 and of Question 6 should be considered.  
A –    
Admissibility  
38      By the second part of Question 2 and by Question 6 respectively, the referring court asks the Court to rule on the validity of Directive 2006/24 and on the interpretation of Article 7(e) of Directive 95/46, so as to enable it to assess whether the retention of certain data relating to the users of the internet sites, laid down by European Union and German legislation, is lawful.  
39      It should be recalled at the outset that although, in view of the division of responsibilities in the preliminary-ruling procedure, it is for the referring court alone to determine the subject-matter of the questions which it proposes to refer to the Court, the Court has held that, in exceptional circumstances, it will examine the conditions in which the case was referred to it by the national court, in order to assess whether it has jurisdiction (Case C-567/07   
Woningstichting Sint Servatius  
 [2009] ECR I-9021, paragraph 42).  
40      That is the case in particular where the problem referred to the Court is purely hypothetical or where the interpretation or consideration of the validity of a rule of European Union law which is sought by the national court has no relation to the actual facts of the main action or to its purpose (see, to that effect, Case C-415/93   
Bosman  
 [1995] ECR I-4921, paragraph 61; Case C-466/04   
Acereda Herrera  
 [2006] ECR I-5341, paragraph 48; Case C-380/05   
Centro Europa 7  
 [2008] ECR I-349, paragraph 53; and   
Woningstichting Sint Servatius  
, paragraph 43).  
41      According to the decisions for reference, the applicants in the main proceedings each brought proceedings before the referring court against the publication under Regulations No 1290/2005 and No 259/2008 of data relating to them. Their applications seek for the   
Land  
 of Hesse to refrain from transmitting or publishing, or to refuse to transmit or publish, the information concerning the aid which they have received from the EAGF and the EAFRD.  
42      The second part of Question 2 and Question 6 have no relation to the subject-matter of the disputes in the main proceedings. They relate, not to the publication of data relating to the beneficiaries of aid under those Funds, such as the applicants in the main proceedings, but to the retention of data relating to persons consulting websites. Since consideration of the second part of Question 2 and Question 6 is therefore of no relevance for the outcome of the main proceedings, there is no need to answer them.  
B –    
Substance  
1.     Question 1 and the first part of Question 2  
a)     Preliminary observations  
43      By Question 1 and the first part of Question 2, the national court asks the Court to examine the validity, first, of Article 44a of Regulation No 1290/2005 and of Regulation No 259/2008 containing the detailed rules for the application of the publication obligation laid down by Article 44a and, second, of Article 42(8b) of Regulation No 1290/2005, the provision which is the legal basis of Regulation No 259/2008.  
44      The referring court considers that the obligation to publish data relating to the beneficiaries of aid from the EAGF and the EAFRD, which follows from the provisions cited in the previous paragraph, constitutes an unjustified interference with the fundamental right to the protection of personal data. It refers essentially to Article 8 of the Convention.  
45      In accordance with Article 6(1) TEU, the European Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union (‘the Charter’), ‘which shall have the same legal value as the Treaties’.  
46      In those circumstances, the validity of Articles 42(8b) and 44a of Regulation No 1290/2005 and of Regulation No 259/2008 must be assessed in the light of the provisions of the Charter.  
47      In this regard, Article 8(1) of the Charter states that ‘[e]veryone has the right to the protection of personal data concerning him or her’. That fundamental right is closely connected with the right to respect of private life expressed in Article 7 of the Charter.  
48      The right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society (see, to that effect, Case C-112/00   
Schmidberger  
 [2003] ECR I-5659, paragraph 80 and the case-law cited).  
49      Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied. It provides that personal data ‘must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.  
50      Moreover, Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.  
51      Finally, according to Article 52(3) of the Charter, in so far as it contains rights which correspond to rights guaranteed by the Convention, the meaning and scope of those rights are to be the same as those laid down by the Convention. Article 53 of the Charter further states that nothing in the Charter is to be interpreted as restricting or adversely affecting the rights recognised inter alia by the Convention.  
52      In those circumstances, it must be considered that the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (see, in particular, European Court of Human Rights,   
Amann v. Switzerland  
 [GC], no. 27798/95, § 65, ECHR 2000-II, and   
Rotaru v. Romania  
 [GC], no. 28341/95, § 43, ECHR 2000-V) and the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention.  
b)     The validity of Article 44a of Regulation No 1290/2005 and of Regulation No 259/2008  
53      It must be recalled, in the first place, that the publication required by Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 implementing that article identifies by name all beneficiaries of aid from the EAGF and the EAFRD, among whom are both natural and legal persons. Having regard to the observations in paragraph 52 above, legal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons.  
54      That is the case with the applicant in the main proceedings in Case C-92/09. The official title of the partnership in question directly identifies natural persons who are its partners.  
55      In the second place, it must be ascertained whether Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 interfere with the rights guaranteed by Articles 7 and 8 of the Charter to beneficiaries of aid from the EAGF or the EAFRD who are identified or identifiable natural persons (‘the beneficiaries concerned’), and, if so, whether such an interference is justified having regard to Article 52 of the Charter.  
i)     Existence of an interference with the rights recognised by Articles 7 and 8 of the Charter  
56      Article 44a of Regulation No 1290/2005 requires the Member States to ensure the annual   
ex-post  
 publication of the names of the beneficiaries of aid from the EAGF and the EAFRD and the amounts received by each beneficiary from each of those Funds. It follows from recital 14 in the preamble to Regulation No 1437/2007 amending Regulation No 1290/2005 that that information must be the subject of ‘general publication’.  
57      Article 1(1)(d) of Regulation No 259/2008 lays down the content of the publication and prescribes that, in addition to the matters mentioned in the preceding paragraph and other information regarding the aid received, ‘the municipality where the beneficiary resides or is registered and, where available, the postal code or the part thereof identifying the municipality’ must be published. Article 2 of that regulation prescribes that the information is to be made available on a single website per Member State and may be consulted by means of a search tool.  
58      It is not disputed that the amounts which the beneficiaries concerned receive from the EAGF and the EAFRD represent part of their income, often a considerable part. Because the information becomes available to third parties, publication on a website of data naming those beneficiaries and indicating the precise amounts received by them thus constitutes an interference with their private life within the meaning of Article 7 of the Charter (see, to that effect,   
Österreichischer Rundfunk and Others  
, paragraphs 73 and 74).  
59      It is of no relevance in this respect that the data published concerns activities of a professional nature (see   
Österreichischer Rundfunk and Others  
, paragraphs 73 and 74). The European Court of Human Rights has held on this point, with reference to the interpretation of Article 8 of the Convention, that the term ‘private life’ must not be interpreted restrictively and that ‘there is no reason of principle to justify excluding activities of a professional … nature from the notion of “private life”’ (see, inter alia,   
Amann v. Switzerland  
, § 65, and   
Rotaru v. Romania  
, § 43).  
60      Moreover, the publication required by Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 constitutes the processing of personal data falling under Article 8(2) of the Charter.  
61      The   
Land  
 of Hesse casts doubt, however, on the very existence of an interference with the private life of the applicants in the main proceedings, as they were informed in the aid application form of the mandatory publication of the data relating to them and, in accordance with Article 8(2) of the Charter, gave their consent to that publication by submitting their applications.  
62      On this point, it should be noted that Article 42(8b) of Regulation No 1290/2005 provides only that ‘the beneficiaries of funds are informed that these data [concerning them, namely their names and the amounts received from each of the Funds] may be made public’. Article 4(1) of Regulation No 259/2008 contains a similar provision, stating that ‘Member States shall inform the beneficiaries that their data will be made public’.  
63      The European Union legislation in question, which merely provides that beneficiaries of aid are to be informed in advance that the data concerning them will be published, thus does not seek to base the personal data processing for which it provides on the consent of the beneficiaries concerned. Furthermore, it must be noted that in the main proceedings, in their aid application forms, the applicants stated only that they were ‘aware that Article 44a of Regulation … No 1290/2005 requires publication of information on the beneficiaries of [funds from] the EAGF and the EAFRD’.  
64      Since the publication of data by name relating to the beneficiaries concerned and the precise amounts received by them from the EAGF and the EAFRD constitutes an interference, as regards those beneficiaries, with the rights recognised by Articles 7 and 8 of the Charter, and since such processing of personal data is not based on the consent of those beneficiaries, it is necessary to examine whether the interference is justified having regard to Article 52(1) of the Charter.  
ii)  Justification of the interference with the rights recognised by Articles 7 and 8 of the Charter  
65      Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms, and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.  
66      First, it is common ground that the interference arising from the publication on a website of data by name relating to the beneficiaries concerned must be regarded as ‘provided for by law’ within the meaning of Article 52(1) of the Charter. Articles 1(1) and 2 of Regulation No 259/2008 expressly provide for such publication.  
67      Second, on the question whether that interference meets an objective of general interest recognised by the European Union within the meaning of Article 52(1) of the Charter, it follows from recital 14 in the preamble to Regulation No 1437/2007 amending Regulation No 1290/2005 and from recital 6 in the preamble to Regulation No 259/2008 that publication of the names of the beneficiaries of aid from the EAGF and the EAFRD and of the amounts which they receive from those Funds is intended to ‘[enhance] transparency regarding the use of Community funds in the [CAP] and [improve] the sound financial management of these funds, in particular by reinforcing public control of the money used’.  
68      The principle of transparency is stated in Articles 1 TEU and 10 TEU and in Article 15 TFEU. It enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system (see Case C-41/00 P   
Interporc  
 v   
Commission  
 [2003] ECR I-2125, paragraph 39, and Case C-28/08 P   
Commission  
 v   
Bavarian Lager  
 [2010] ECR I-0000, paragraph 54).  
69      By reinforcing public control of the use of the money from the EAGF and the EAFRD, the publication required by the provisions whose validity is contested contributes to the appropriate use of public funds by the administration (see, to that effect,   
Österreichischer Rundfunk and Others  
, paragraph 81).  
70      Moreover, that publication relating to the use of money paid out by the agricultural Funds will enable citizens to participate more closely in the public debate surrounding decisions on the direction to be taken by the CAP.  
71      Consequently, by aiming to increase the transparency of the use of funds in the context of the CAP, Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 pursue an objective of general interest recognised by the European Union.  
72      Third, it is also necessary to ascertain whether the limitation imposed on the rights conferred by Articles 7 and 8 of the Charter is proportionate to the legitimate aim pursued (see, inter alia, European Court of Human Rights,   
Gillow v. United Kingdom  
, 24 November 1986, § 55, Series A no. 109, and   
Österreichischer Rundfunk and Others  
, paragraph 83).  
73      The applicants in the main proceedings observe that the data whose publication is provided for in Article 44a of Regulation No 1290/2005 and in Regulation No 259/2008 allows third parties to draw conclusions as to their income. They explain that the aid represents between 30% and 70% of the total income of the beneficiaries concerned. The legitimate interests of the public would, they argue, be satisfied by the publication of anonymous statistics.  
74      It is settled case-law that the principle of proportionality, which is one of the general principles of European Union law, requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it (Case C-58/08   
Vodafone and Others  
 [2010] ECR I-0000, paragraph 51 and the case-law cited).  
75      It is not disputed that the publication on the internet of data by name relating to the beneficiaries concerned and the precise amounts received by them from the EAGF and the EAFRD is liable to increase transparency with respect to the use of the agricultural aid concerned. Such information made available to citizens reinforces public control of the use to which that money is put and contributes to the best use of public funds.  
76      As to whether the measure is necessary, it must be recalled that the objective of the publication at issue may not be pursued without having regard to the fact that that objective must be reconciled with the fundamental rights set forth in Articles 7 and 8 of the Charter (see, to that effect, Case C-73/07   
Satakunnan Markkinapörssi and Satamedia  
 [2008] ECR I-9831, paragraph 53).  
77      It is thus necessary to determine whether the Council of the European Union and the Commission balanced the European Union’s interest in guaranteeing the transparency of its acts and ensuring the best use of public funds against the interference with the right of the beneficiaries concerned to respect for their private life in general and to the protection of their personal data in particular. The Court has held in this respect that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (  
Satakunnan Markkinapörssi and Satamedia  
, paragraph 56).  
78      The Member States which have submitted written observations to the Court, the Council and the Commission argue that the objective pursued by the publication required by Article 44a of Regulation No 1290/2005 and by Regulation No 259/2008 could not be achieved by measures which interfere less with the right of the beneficiaries concerned to respect for their private life in general and the protection of their personal data in particular. Information limited to those of the beneficiaries concerned who receive aid exceeding a certain threshold would, it is submitted, not give taxpayers an accurate image of the CAP. Taxpayers would have the impression that there were only ‘big’ beneficiaries of aid from the agricultural Funds, whereas there are numerous ‘little’ ones. Limiting publication to legal persons only would not be satisfactory either. The Commission submits in this connection that the largest beneficiaries of agricultural aid include natural persons.  
79      While it is true that in a democratic society taxpayers have a right to be kept informed of the use of public funds (  
Österreichischer Rundfunk and Others  
, paragraph 85), the fact remains that striking a proper balance between the various interests involved made it necessary for the institutions, before adopting the provisions whose validity is contested, to ascertain whether publication via a single freely consultable website in each Member State of data by name relating to all the beneficiaries concerned and the precise amounts received by each of them from the EAGF and the EAFRD – with no distinction being drawn according to the duration, frequency or nature and amount of the aid received – did not go beyond what was necessary for achieving the legitimate aims pursued, having regard in particular to the interference with the rights guaranteed by Articles 7 and 8 of the Charter resulting from such publication.  
80      As far as natural persons benefiting from aid under the EAGF and the EAFRD are concerned, however, it does not appear that the Council and the Commission sought to strike such a balance between the European Union’s interest in guaranteeing the transparency of its acts and ensuring the best use of public funds, on the one hand, and the fundamental rights enshrined in Articles 7 and 8 of the Charter, on the other.  
81      There is nothing to show that, when adopting Article 44a of Regulation No 1290/2005 and Regulation No 259/2008, the Council and the Commission took into consideration methods of publishing information on the beneficiaries concerned which would be consistent with the objective of such publication while at the same time causing less interference with those beneficiaries’ right to respect for their private life in general and to protection of their personal data in particular, such as limiting the publication of data by name relating to those beneficiaries according to the periods for which they received aid, or the frequency or nature and amount of aid received.  
82      Such limited publication by name might be accompanied, if appropriate, by relevant information about other natural persons benefiting from aid under the EAGF and the EAFRD and the amounts received by them.  
83      The institutions ought thus to have examined, in the course of striking a proper balance between the various interests involved, whether publication by name limited in the manner indicated in paragraph 81 above would have been sufficient to achieve the objectives of the European Union legislation at issue in the main proceedings. In particular, it does not appear that such a limitation, which would protect some of the beneficiaries concerned from interference with their private lives, would not provide citizens with a sufficiently accurate image of the aid granted by the EAGF and the EAFRD to achieve the objectives of that legislation.  
84      The Member States which submitted written observations to the Court and the Council and the Commission refer also to the significant role of the CAP in the European Union budget in order to justify the need for publication laid down by Article 44a of Regulation No 1290/2005 and by Regulation No 259/2008.  
85      That argument must be rejected. It is necessary to bear in mind that the institutions are obliged to balance, before disclosing information relating to a natural person, the European Union’s interest in guaranteeing the transparency of its actions and the infringement of the rights recognised by Articles 7 and 8 of the Charter. No automatic priority can be conferred on the objective of transparency over the right to protection of personal data (see, to that effect,   
Commission   
v   
Bavarian Lager  
, paragraphs 75 to 79), even if important economic interests are at stake.  
86      It follows from the foregoing that it does not appear that the institutions properly balanced, on the one hand, the objectives of Article 44a of Regulation No 1290/2005 and of Regulation No 259/2008 against, on the other, the rights which natural persons are recognised as having under Articles 7 and 8 of the Charter. Regard being had to the fact that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (  
Satakunnan Markkinapörssi and Satamedia  
, paragraph 56) and that it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives of the European Union rules in question, it must be held that, by requiring the publication of the names of all natural persons who were beneficiaries of EAGF and EAFRD aid and of the exact amounts received by those persons, the Council and the Commission exceeded the limits which compliance with the principle of proportionality imposes.  
87      Finally, with regard to the legal persons which received EAGF and EAFRD aid, and in so far as they may invoke the rights conferred by Articles 7 and 8 of the Charter (see paragraph 53 of the present judgment), the view must be taken that the obligation to publish which follows from the provisions of the European Union rules the validity of which has here been brought into question does not go beyond the limits imposed by compliance with the principle of proportionality. The seriousness of the breach of the right to protection of personal data manifests itself in different ways for, on the one hand, legal persons and, on the other, natural persons. It is necessary to point out in this regard that legal persons are already subject to a more onerous obligation in respect of the publication of data relating to them. Furthermore, the obligation on the competent national authorities to examine, before the data in question are published and for each legal person which is a beneficiary of EAGF or EAFRD aid, whether the name of that person identifies natural persons would impose on those authorities an unreasonable administrative burden (see, to that effect, judgment of the European Court of Human Rights,   
K.U. v.  
Finland  
, 2 March 2009, application no 2872/02, § 48, not yet published).  
88      In those circumstances, it must be held that the provisions of European Union law, the validity of which is questioned by the referring court, observe, in so far as they concern the publication of data relating to legal persons, a fair balance in the consideration taken of the respective interests in issue.  
89      On the basis of all of the foregoing, Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 must be declared invalid to the extent to which, with regard to natural persons who are beneficiaries of EAGF and EAFRD aid, those provisions impose an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons have received such aid, the frequency of such aid or the nature and amount thereof.   
c)     The validity of Article 42(8b) of Regulation No 1290/2005  
90      Article 42(8b) of Regulation No 1290/2005 authorises the Commission to adopt the detailed rules for the implementation solely of Article 44a of that regulation.  
91      However, as Article 44a of Regulation No 1290/2005 has to be declared invalid for the reasons indicated above, Article 42(8b) of that regulation must be declared invalid in like manner.  
92      The answer to the first question and to the first part of the second question is therefore that Articles 42(8b) and 44a of Regulation No 1290/2005, and Regulation No 259/2008, are invalid in so far as, with regard to natural persons who are beneficiaries of EAGF and EAFRD aid, those provisions impose an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons have received such aid, the frequency of such aid or the nature and amount thereof.   
d)     The effects in time of the invalidity which has been established  
93      Where it is justified by overriding considerations of legal certainty, the second paragraph of Article 264 TFEU, which is also applicable by analogy to a reference under Article 267 TFEU for a preliminary ruling on the validity of acts of the European Union, confers on the Court a discretion to decide, in each particular case, which specific effects of the act in question must be regarded as definitive (see, to that effect, Case C-333/07   
Regie Networks  
 [2008] ECR I-10807, paragraph 121 and the case-law cited).  
94      In view of the large number of publications which have taken place in the Member States on the basis of rules which were regarded as being valid, it must be held that the invalidity of the provisions mentioned in paragraph 92 of the present judgment does not allow any action to be brought to challenge the effects of the publication of the lists of beneficiaries of EAGF and EAFRD aid carried out by the national authorities on the basis of those provisions during the period prior to the date on which the present judgment is delivered.   
2.     The third question  
95      By its third question, the referring court seeks, essentially, to ascertain whether the second indent of Article 18(2) of Directive 95/46 is to be interpreted as meaning that the publication of the information resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008 may be effected only if the personal data protection official has, prior to such publication, kept a full register within the terms of the second indent of Article 18(2).   
96      It must, in this regard, be borne in mind that Article 18(1) of Directive 95/46 establishes the principle that the supervisory authority must be notified before any wholly or partly automatic operation for the processing of personal data, or any set of such operations intended to serve a single purpose or several related purposes, is carried out. As recital 48 in the preamble to Directive 95/46 explains, ‘the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive’.   
97      The second indent of Article 18(2) of Directive 95/46, however, provides that Member States may provide for the simplification of or exemption from that obligation in the case where, inter alia, the controller appoints a personal data protection official. It appears from the decisions for reference that such an appointment was made in the   
Land   
of Hesse so far as concerns the publication of data resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008.   
98      According to the second indent of Article 18(2) of Directive 95/46, a personal data protection official has a number of tasks which are designed to ensure that processing operations are unlikely to have an adverse effect on the rights and freedoms of the persons concerned. The official is thus responsible for, among other things, ‘keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2) [of Directive 95/46]’. The latter provision refers to Article 19(1)(a) to (e) of Directive 95/46.  
99      However, contrary to the view expressed by the referring court, the second indent of Article 18(2) of Directive 95/46 does not require any provision to be adopted which imposes an obligation on the personal data protection official to maintain a register containing the information referred to in Article 21(2) of that directive, read in conjunction with Article 19(1)(a) to (e) thereof, before the processing of the data concerned is undertaken. The register referred to in the second indent of Article 18(2) of Directive 95/46 need contain only ‘processing operations carried out’.   
100    In those circumstances, the absence, established by the referring court, of a full register prior to the data processing cannot affect the legality of a publication such as that resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008.  
101    The answer to the third question is therefore that the second indent of Article 18(2) of Directive 95/46 must be interpreted as not placing the personal data protection official under an obligation to keep the register provided for by that provision before an operation for the processing of personal data, such as that resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008, is carried out.  
3.     The fourth question  
102    By its fourth question, the referring court seeks, essentially, to ascertain whether Article 20 of Directive 95/46 is to be interpreted as making the publication of the information resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008 subject to the prior checks for which that Article 20 provides.   
103    It must first be pointed out that Article 20(1) of Directive 95/46 provides that ‘Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof’.  
104    It follows that Directive 95/46 does not make the processing of personal data subject, in general, to a prior check. As is clear from recital 52 in the preamble to Directive 95/46, the European Union legislature took the view that ‘  
ex post facto  
 verification by the competent authorities must in general be considered a sufficient measure’.  
105    With regard to processing operations which are subject to prior checks, that is to say, processing operations which are likely to pose specific risks to the rights and freedoms of data subjects, recital 53 in the preamble to Directive 95/46 states that processing operations are likely to pose such risks ‘by virtue of their nature, their scope or their purposes’. Even though Member States have the option of specifying in greater detail in their legislation the processing operations which may pose specific risks to the rights and freedoms of data subjects, Directive 95/46 provides, as is evident from recital 54 in its preamble, that the number of such operations ‘should be very limited’.   
106    It must further be pointed out that, under Article 27(1) of Regulation No 45/2001, processing operations which are likely to present specific risks to the rights and freedoms of data subjects are also subject to prior checking when carried out by institutions and bodies of the European Union. Article 27(2) of that regulation specifies the operations which are likely to present such risks. In view of the parallel relationship between the provisions of Directive 95/46 and those of Regulation No 45/2001 which relate to prior checks, the listing in Article 27(2) of Regulation No 45/2001 of the processing operations which are likely to present specific risks to the rights and freedoms of data subjects must be considered relevant for the purpose of interpreting Article 20 of Directive 95/46.  
107    However, it does not appear that the publication of the data imposed by Articles 42(8b) and 44a of Regulation No 1290/2005 and by Regulation No 259/2008 comes within any of the categories of processing operations covered by Article 27(2) of Regulation No 45/2001.  
108    In those circumstances, the answer to the fourth question is that Article 20 of Directive 95/46 must be interpreted as not imposing an obligation on the Member States to make the publication of information resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008 subject to the prior checks for which that Article 20 provides.  
109    In view of the answer to the fourth question, there is no longer any need to answer the fifth question.  
IV –    
Costs  
110    Since these proceedings are, for the parties to the main proceedings, a step in the actions pending before the national court, the decisions on costs are a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Articles 42(8b) and 44a of Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, as amended by Council Regulation (EC) No 1437/2007 of 26 November 2007, and Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Regulation No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) are invalid in so far as, with regard to natural persons who are beneficiaries of EAGF and EAFRD aid, those provisions impose an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons have received such aid, the frequency of such aid or the nature and amount thereof.  
2.        
The invalidity of the provisions of European Union law mentioned in paragraph 1 of this operative part does not allow any action to be brought to challenge the effects of the publication of the lists of beneficiaries of EAGF and EAFRD aid carried out by the national authorities on the basis of those provisions during the period prior to the date on which the present judgment is delivered.  
3.        
The second indent of Article 18(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as not placing the personal data protection official under an obligation to keep the register provided for by that provision before an operation for the processing of personal data, such as that resulting from Articles 42(8b) and 44a of Regulation No 1290/2005, as amended by Regulation No 1437/2007, and from Regulation No 259/2008, is carried out.  
4.        
Article 20 of Directive 95/46 must be interpreted as not imposing an obligation on the Member States to make the publication of information resulting from Articles 42(8b) and 44a of Regulation No 1290/2005, as amended by Regulation No 1437/2007, and from Regulation No 259/2008 subject to the prior checks for which that Article 20 provides.

ID: ab32c96b-8197-4131-93a0-b2e5174d6228

Judgment of 6 Oct 2020, C-511/18 (  
La Quadrature du Net and others  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Location data   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
   
JUDGMENT OF THE COURT (Grand Chamber)  
6 October 2020 (\*)  
Table of Contents  
Legislative framework  
EU law  
Directive 95/46  
Directive 97/66  
Directive 2000/31  
Directive 2002/21  
Directive 2002/58  
Regulation 2016/679  
French law  
Code de la sécurité intérieure (Internal Security Code)  
The CPCE  
Loi n° 2004 575 du 21 juin 2004 pour la confiance dans l’économie numérique (Law No 2004575 of 21 June 2004 to promote trust in the digital economy)  
Decree No 2011 219  
Belgian law  
The disputes in the main proceedings and the questions referred for a preliminary ruling  
Case C 511/18  
Case C 512/18  
Case C 520/18  
Procedure before the Court  
Consideration of the questions referred  
Question 1 in Cases C 511/18 and C512/18 and questions 1 and 2 in Case C520/18  
Preliminary remarks  
Scope of Directive 2002/58  
Interpretation of Article 15(1) of Directive 2002/58  
– Legislative measures providing for the preventive retention of traffic and location data for the purpose of safeguarding national security  
– Legislative measures providing for the preventive retention of traffic and location data for the purposes of combating crime and safeguarding public security  
– Legislative measures providing for the preventive retention of IP addresses and data relating to civil identity for the purposes of combating crime and safeguarding public security  
– Legislative measures providing for the expedited retention of traffic and location data for the purpose of combating serious crime  
Questions 2 and 3 in Case C 511/18  
Automated analysis of traffic and location data  
Real-time collection of traffic and location data  
Notification of persons whose data has been collected or analysed  
Question 2 in Case C 512/18  
Question 3 in Case C 520/18  
Costs  
(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Providers of electronic communications services – Hosting service providers and Internet access providers – General and indiscriminate retention of traffic and location data – Automated analysis of data – Real-time access to data – Safeguarding national security and combating terrorism – Combating crime – Directive 2002/58/EC – Scope – Article 1(3) and Article 3 – Confidentiality of electronic communications – Protection – Article 5 and Article 15(1) – Directive 2000/31/EC – Scope – Charter of Fundamental Rights of the European Union – Articles 4, 6, 7, 8 and 11 and Article 52(1) – Article 4(2) TEU)  
In Joined Cases C-511/18, C-512/18 and C-520/18,  
REQUESTS for a preliminary ruling under Article 267 TFEU from the Conseil d’État (Council of State, France), made by decisions of 26 July 2018, received at the Court on 3 August 2018 (C-511/18 and C-512/18), and from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 19 July 2018, received at the Court on 2 August 2018 (C-520/18), in the proceedings  
La Quadrature du Net  
 (C-511/18 and C-512/18),  
French Data Network   
(C-511/18 and C-512/18),  
Fédération des fournisseurs d’accès à Internet associatifs  
 (C-511/18 and C-512/18),  
Igwan.net   
(C-511/18)  
v  
Premier ministre  
 (C-511/18 and C-512/18),  
Garde des Sceaux, ministre de la Justice   
(C-511/18 and C-512/18),  
Ministre de l’Intérieur   
(C-511/18),  
Ministre des Armées  
 (C-511/18),  
interveners:  
Privacy International  
 (C-512/18),  
Center for Democracy and Technology   
(C-512/18),  
and  
Ordre des barreaux francophones et germanophone,  
Académie Fiscale ASBL,  
UA,  
Liga voor Mensenrechten ASBL,  
Ligue des Droits de l’Homme ASBL,  
VZ,  
WY,  
XX  
v  
Conseil des ministres  
,  
interveners:  
Child Focus  
 (C-520/18),  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb and L.S. Rossi, Presidents of Chambers, J. Malenovský, L. Bay Larsen, T. von Danwitz (Rapporteur), C. Toader, K. Jürimäe, C. Lycourgos and N. Piçarra, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 9 and 10 September 2019,  
after considering the observations submitted on behalf of:  
–        La Quadrature du Net, the Fédération des fournisseurs d’accès à Internet associatifs, Igwan.net and the Center for Democracy and Technology, by A. Fitzjean Ò Cobhthaigh, avocat,  
–        French Data Network, by Y. Padova, avocat,  
–        Privacy International, by H. Roy, avocat,  
–        the Ordre des barreaux francophones et germanophone, by E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart and J.-F. Henrotte, avocats,  
–        the Académie Fiscale ASBL and UA, by J.-P. Riquet,  
–        the Liga voor Mensenrechten ASBL, by J. Vander Velpen, avocat,  
–        the Ligue des Droits de l’Homme ASBL, by R. Jespers and J. Fermon, avocats,  
–        VZ, WY and XX, by D. Pattyn, avocat,  
–        Child Focus, by N. Buisseret, K. De Meester and J. Van Cauter, avocats,  
–        the French Government, initially by D. Dubois, F. Alabrune, D. Colas, E. de Moustier and A.-L. Desjonquères, then by D. Dubois, F. Alabrune, E. de Moustier and A.-L. Desjonquères, acting as Agents,  
–        the Belgian Government, by J.-C. Halleux, P. Cottin and C. Pochet, acting as Agents, and by J. Vanpraet, Y. Peeters, S. Depré and E. de Lophem, avocats,  
–        the Czech Government, by M. Smolek, J. Vláčil and O. Serdula, acting as Agents,  
–        the Danish Government, initially by J. Nymann-Lindegren, M. Wolff and P. Ngo, then by J. Nymann-Lindegren and M. Wolff, acting as Agents,  
–        the German Government, initially by J. Möller, M. Hellmann, E. Lankenau, R. Kanitz and T. Henze, then by J. Möller, M. Hellmann, E. Lankenau and R. Kanitz, acting as Agents,  
–        the Estonian Government, by N. Grünberg and A. Kalbus, acting as Agents,  
–        Ireland, by A. Joyce, M. Browne and G. Hodge, acting as Agents, and by D. Fennelly, Barrister-at-Law,  
–        the Spanish Government, initially by L. Aguilera Ruiz and A. Rubio González, then by L. Aguilera Ruiz, acting as Agent,  
–        the Cypriot Government, by E. Neofytou, acting as Agent,  
–        the Latvian Government, by V. Soņeca, acting as Agent,  
–        the Hungarian Government, initially by M.Z. Fehér and Z. Wagner, then by M.Z. Fehér, acting as Agent,  
–        the Netherlands Government, by M.K. Bulterman and M.A.M. de Ree, acting as Agents,  
–        the Polish Government, by B. Majczyna, J. Sawicka and M. Pawlicka, acting as Agents,  
–        the Swedish Government, initially by H. Shev, H. Eklinder, C. Meyer-Seitz and A. Falk, then by H. Shev, H. Eklinder, C. Meyer-Seitz and J. Lundberg, acting as Agents,  
–        the United Kingdom Government, by S. Brandon, acting as Agent, and by G. Facenna QC and C. Knight, Barrister,  
–        the Norwegian Government, by J. Vangsnes, acting as Agent,  
–        the European Commission, initially by H. Kranenborg, M. Wasmeier and P. Costa de Oliveira, then by H. Kranenborg and M. Wasmeier, acting as Agents,  
–        the European Data Protection Supervisor, by T. Zerdick and A. Buchta, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 15 January 2020,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), and of Articles 12 to 15 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) (OJ 2000 L 178, p. 1), read in the light of Articles 4, 6, 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’) and Article 4(2) TEU.  
2        The request in Case C-511/18 has been made in proceedings between La Quadrature du Net, French Data Network, the Fédération des fournisseurs d’accès à Internet associatifs and Igwan.net, on the one hand, and the Premier ministre (Prime Minister, France), the Garde des Sceaux, ministre de la Justice (Keeper of the Seals, Minister for Justice, France), the ministre de l’Intérieur (Minister for the Interior, France) and the ministre des Armées (Minister for the Armed Forces, France), on the other, concerning the lawfulness of: décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (Decree No 2015-1185 of 28 September 2015 designating specialised intelligence services) (  
Journal Officiel de la République Française  
 (JORF) of 29 September 2015, text 1 of 97; ‘Decree No 2015-1185’); décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l’État (Decree No 2015-1211 of 1 October 2015 on litigation relating to the implementation of intelligence techniques subject to authorisation and files on matters of State security) (JORF of 2 October 2015, text 7 of 108; ‘Decree No 2015-1211’), décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l’article L. 811-4 du code de la sécurité intérieure (Decree No 2015-1639 of 11 December 2015 on the designation of services other than the specialist intelligence services which are authorised to use the techniques referred to in Title V of Book VIII of the Internal Security Code, adopted pursuant to Article L. 811-4 thereof) (JORF of 12 December 2015, text 28 of 127; ‘Decree No 2015-1639’), and décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Decree No 2016-67 of 29 January 2016 on intelligence gathering techniques) (JORF of 31 January 2016, text 2 of 113; ‘Decree No 2016-67’).  
3        The request in Case C-512/18 has been made in proceedings between French Data Network, La Quadrature du Net and the Fédération des fournisseurs d’accès à Internet associatifs, on the one hand, and the Prime Minister (France) and the Keeper of the Seals, Minister for Justice (France), on the other, concerning the lawfulness of Article R. 10-13 of the code des postes et des communications électroniques (Post and Electronic Communications Code; ‘the CPCE’) and décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d’identifier toute personne ayant contribué à la création d’un contenu mis en ligne (Decree No 2011-219 of 25 February 2011 on the retention and communication of data that can be used to identify any person having assisted in the creation of content posted online) (JORF of 1 March 2011, text 32 of 170; ‘Decree No 2011-219’).  
4        The request in Case C-520/18 has been made in proceedings between the Ordre des barreaux francophones et germanophone, the Académie Fiscale ASBL, UA, the Liga voor Mensenrechten ASBL, the Ligue des Droits de l’Homme ASBL, VZ, WY and XX, on the one hand, and the Conseil des ministres (Council of Ministers, Belgium), on the other, concerning the lawfulness of the loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (Law of 29 May 2016 on the collection and retention of data in the electronic telecommunications sector) (  
Moniteur belge  
 of 18 July 2016, p. 44717; ‘the Law of 29 May 2016’).  
   
Legislative framework  
   
EU law  
   
Directive 95/46  
5        Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) was repealed with effect from 25 May 2018 by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (OJ 2016 L 119, p 1). Article 3(2) of Directive 95/46 provided:  
‘This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household act.’  
6        Article 22 of Directive 95/46, which is in Chapter III of that directive, headed ‘Judicial remedies, liability and sanctions’, was worded as follows:  
‘Without prejudice to any administrative remedy for which provision may be made,   
inter alia  
 before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.’  
   
Directive 97/66  
7        Under Article 5 of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24, p. 1), headed ‘Confidentiality of the communications’:  
‘1.      Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14(1).  
2.      Paragraph 1 shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.’  
   
Directive 2000/31  
8        Recitals 14 and 15 of Directive 2000/31 provide:  
‘(14)      The protection of individuals with regard to the processing of personal data is solely governed by Directive [95/46] and Directive [97/66] which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.  
(15)      The confidentiality of communications is guaranteed by Article 5 Directive [97/66]; in accordance with that Directive, Member States must prohibit any kind of interception or surveillance of such communications by others than the senders and receivers, except when legally authorised.’  
9        Article 1 of Directive 2000/31 is worded as follows:  
‘1.      This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.  
2.      This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.  
3.      This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.  
…  
5.      This Directive shall not apply to:  
…  
(b)      questions relating to information society services covered by Directives [95/46] and [97/66];  
…’  
10      Article 2 of Directive 2000/31 is worded as follows:  
‘For the purpose of this Directive, the following terms shall bear the following meanings:  
(a)      “information society services”: services within the meaning of Article 1(2) of Directive 98/34/EC [of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations (OJ 1998 L 204, p. 37)] as amended by Directive 98/48/EC [of the European Parliament and of the Council of 20 July 1998 (OJ 1998 L 217, p. 18)];  
…’  
11      Article 15 of Directive 2000/31 provides:  
‘1.      ‘Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.  
2.      Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.’  
   
Directive 2002/21  
12      Recital 10 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ 2002 L 108, p. 33) states:  
‘The definition of “information society service” in Article 1 of Directive [98/34, as amended by Directive 98/48,] spans a wide range of economic activities which take place on-line. Most of these activities are not covered by the scope of this Directive because they do not consist wholly or mainly in the conveyance of signals on electronic communications networks. Voice telephony and electronic mail conveyance services are covered by this Directive. The same undertaking, for example an Internet service provider, can offer both an electronic communications service, such as access to the Internet, and services not covered under this Directive, such as the provision of web-based content.’  
13      Article 2 of Directive 2002/21 provides:  
‘For the purposes of this Directive:  
…  
(c)      “electronic communications service” means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive [98/34], which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;  
…’  
   
Directive 2002/58  
14      Recitals 2, 6, 7, 11, 22, 26 and 30 of Directive 2002/58 state:  
‘(2)      This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the [Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.  
…  
(6)      The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.  
(7)      In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.  
…  
(11)      Like Directive [95/46], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [Union] law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, [signed in Rome on 4 November 1950,] as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.  
…  
(22)      The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. …  
…  
(26)      The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data … may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber’s right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services … should also be erased or made anonymous …  
…  
(30)      Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. …’  
15      Article 1 of Directive 2002/58, headed ‘Scope and aim’, provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the [European Union].  
2.      The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.  
3.      This Directive shall not apply to activities which fall outside the scope of the [TFEU], such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.’  
16      Article 2 of Directive 2002/58, headed ‘Definitions’, provides:  
‘Save as otherwise provided, the definitions in Directive [95/46] and in Directive [2002/21] shall apply.  
The following definitions shall also apply:  
(a)      “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  
(c)      “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
…’  
17      Article 3 of Directive 2002/58, headed ‘Services concerned’, provides:  
‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.’  
18      Article 5 of Directive 2002/58, headed ‘Confidentiality of the communications’, provides:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
…  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
19      Article 6 of Directive 2002/58, headed ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
…’  
20      Article 9(1) of that directive, that article being headed ‘Location data other than traffic data’, provides:  
‘Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …’  
21      Article 15 of that directive, headed ‘Application of certain provisions of Directive [95/46]’, states:  
‘1.      Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may,   
inter alia  
, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of [Union] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.  
…  
2.      The provisions of Chapter III on judicial remedies, liability and sanctions of Directive [95/46] shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.  
…’  
   
Regulation 2016/679  
22      Recital 10 of Regulation 2016/679 states:  
‘In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …’  
23      Article 2 of that regulation provides:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;  
…  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.  
…  
4.      This Regulation shall be without prejudice to the application of Directive [2000/31], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.’  
24      Article 4 of that regulation reads as follows:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…’  
25      Article 5 of Regulation 2016/679 provides:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (“purpose limitation”);  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);  
(f)      processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).  
…’  
26      Article 6 of that regulation reads as follows:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
…  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
…  
3.      The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.  
The purpose of the processing shall be determined in that legal basis … That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.  
…’  
27      Article 23 of that regulation provides:  
‘1.      Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;  
(e)      other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation … matters, public health and social security;  
(f)      the protection of judicial independence and judicial proceedings;  
(g)      the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;  
(h)      a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);  
(i)      the protection of the data subject or the rights and freedoms of others;  
(j)      the enforcement of civil law claims.  
2.      In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:  
(a)      the purposes of the processing or categories of processing;  
(b)      the categories of personal data;  
(c)      the scope of the restrictions introduced;  
(d)      the safeguards to prevent abuse or unlawful access or transfer;  
(e)      the specification of the controller or categories of controllers;  
(f)      the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;  
(g)      the risks to the rights and freedoms of data subjects; and  
(h)      the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.’  
28      Under Article 79(1) of that regulation:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’  
29      Article 94 of Regulation 2016/679 provides:  
‘1.      Directive [95/46] is repealed with effect from 25 May 2018.  
2.      References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.’  
30      Article 95 of that regulation provides:  
‘This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive [2002/58].’  
   
French law  
   
Code de la sécurité intérieure (Internal Security Code)  
31      Book VIII of the legislative part of the code de la sécurité intérieure (Internal Security Code; ‘the CSI’) lays down rules relating to intelligence in Articles L. 801-1 to L. 898-1.  
32      Article L. 811-3 of the CSI states:  
‘For the sole performance of their respective tasks, the specialised intelligence services may use the techniques referred to in Title V of this Book in order to gather intelligence relating to the protection and promotion of the following fundamental State interests:  
1.      National independence, territorial integrity and national defence;  
2.      Major foreign policy interests, the implementation of France’s European and international commitments and the prevention of all forms of foreign interference;  
3.      France’s major economic, industrial and scientific interests;  
4.      The prevention of terrorism;  
5.      The prevention of:  
(a)      attacks against the republican nature of the institutions;  
(b)      actions designed to maintain or rebuild groups that have been disbanded under Article L. 212-1;  
(c)      collective violence liable to cause serious disruption to the maintenance of law and order;  
6.      The prevention of organised crime;  
7.      The prevention of the proliferation of weapons of mass destruction.’  
33      Article L. 811-4 of the CSI provides:  
‘A decree adopted in the Conseil d’État (Council of State, France) following consultation of the Commission nationale de contrôle des techniques de renseignement (Commission for the Oversight of Intelligence Techniques, France) shall designate the services, other than the specialised intelligence services, within the purview of the Ministers for Defence, the Interior and Justice and the ministers responsible for economic affairs, the budget and customs, which may be authorised to use the techniques referred to in Title V of the present Book under the conditions laid down in this Book. It shall specify, for each service, the purposes mentioned in Article L. 811-3 and the techniques which may be authorised.’  
34      The first paragraph of Article L. 821-1 of the CSI is worded as follows:  
‘The implementation on national territory of the intelligence gathering techniques referred to in Chapters I to IV of Title V of this Book shall be subject to prior authorisation from the Prime Minister following consultation of the Commission for the Oversight of Intelligence Techniques.’  
35      Article L. 821-2 of the CSI provides:  
‘The authorisation mentioned in Article L. 821-1 shall be issued upon a written and reasoned application from the Minister for Defence, the Minister for the Interior, the Minister for Justice or the ministers responsible for economic affairs, the budget or customs. Each minister may delegate that power individually only to immediate staff with clearance to handle confidential material relating to national defence.  
The application shall state:  
1.      the technique(s) to be implemented;  
2.      the service for which it is submitted;  
3.      the purpose(s) pursued;  
4.      the reason(s) for the measures;  
5.      the period of validity of the authorisation;  
6.      the person(s), place(s) or vehicle(s) concerned.  
In respect of point 6, persons whose identity is not known may be designated by their identifiers or status and places or vehicles may be designated by reference to the persons who are the subject of the application.  
…’  
36      Under the first paragraph of Article L. 821-3 of the CSI:  
‘The application shall be sent to the President or, failing that, to one of the members of the Commission for the Oversight of Intelligence Techniques mentioned in points 2 and 3 of Article L. 831-1, who shall provide the Prime Minister with an opinion within 24 hours. If the application is examined by the select panel or the full panel of the Commission, the Prime Minister shall be informed forthwith and the opinion shall be issued within 72 hours.’  
37      Article L. 821-4 of the CSI provides:  
‘Authorisation to implement the techniques referred to in Chapters I to IV of Title V of this Book shall be issued by the Prime Minister for a maximum period of four months. … The authorisation shall contain the grounds and statements set out in points 1 to 6 of Article L. 821-2. All authorisations shall be renewable under the same conditions as those laid down in this Chapter.  
Where the authorisation is issued after obtaining an unfavourable opinion from the Commission for the Oversight of Intelligence Techniques, it shall state the reasons why that opinion was not followed.  
…’  
38      Article L. 833-4 of the CSI, which appears in Chapter III of Title III, provides:  
‘The Commission shall – on its own initiative or after receiving a complaint from any person wishing to verify that no intelligence techniques have been unlawfully implemented against him or her – conduct a review of the technique or techniques referred to with a view to determining whether they have been or are being implemented in accordance with this Book. It shall notify the complainant that the necessary investigations have been carried out, without confirming or denying their implementation.’  
39      The first and second paragraphs of Article L. 841-1 of the CSI read as follows:  
‘Subject to the special provisions set out in Article L. 854-9 of this Code, the Conseil d’État (Council of State, France) shall have jurisdiction to hear, under the conditions laid down in Chapter III bis of Title VII of Book VII of the code de justice administrative (Code of Administrative Justice), actions concerning the implementation of the intelligence techniques referred to in Title V of this Book.  
An action may be brought before it by:  
1.      any person wishing to verify that no intelligence techniques have been unlawfully implemented against him or her and who can demonstrate that the procedure provided for in Article L. 833-4 has been conducted beforehand;  
2.      the Commission for the Oversight of Intelligence Techniques, under the conditions laid down in Article L. 833-8.’  
40      Title V of Book VIII of the legislative part of the CSI, concerning ‘intelligence gathering techniques subject to authorisation’, includes, inter alia, Chapter I, headed ‘Access of the administrative authorities to connection data’, containing Articles L. 851-1 to L. 851-7 of the CSI.  
41      Article L. 851-1 of the CSI provides:  
‘Subject to the conditions laid down in Chapter I of Title II of this Book, the collection of information or documents processed or retained by their networks or electronic communications services, including technical data relating to the identification of the subscription or connection numbers to electronic communications services, the inventorying of the subscription and connection numbers of a specified person, the location of the terminal equipment used and the communications of a subscriber, namely the list of numbers called and calling and the duration and date of the communications, may be authorised from electronic communications operators and the persons referred to in Article L. 34-1 of the [CPCE] as well as from the persons referred to in Article 6(I)(1) and (2) of Loi n.° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique (Law No 2004-575 of 21 June 2004 to promote trust in the digital economy) [(JORF of 22 June 2004, p. 11168)].  
By way of derogation from Article L. 821-2, written and reasoned applications for technical data relating to the identification of subscription or connection numbers to electronic communications services, or the inventorying of all the subscription or connection numbers of a specified person, shall be sent directly to the Commission for the Oversight of Intelligence Techniques by individually designated and authorised agents of the intelligence services referred to in Articles L. 811-2 and L. 811-4. The Commission shall issue its opinion under the conditions laid down in Article L. 821-3.  
A department reporting to the Prime Minister shall be responsible for gathering information or documents from the operators and persons referred to in the first paragraph of this article. The Commission for the Oversight of Intelligence Techniques shall have permanent, complete, direct and immediate access to the information or documents collected.  
The detailed rules for the application of this article shall be laid down by decree adopted in the Conseil d’État (Council of State, France) following consultation of the Commission nationale de l’informatique et des libertés (Data Protection Authority, France) and the Commission for the Oversight of Intelligence Techniques.’  
42      Article L. 851-2 of the CSI provides:  
‘I.      Under the conditions laid down in Chapter I of Title II of this Book, and for the sole purpose of preventing terrorism, the collection in real time, on the networks of the operators and persons referred to in Article L. 851-1, of the information or documents referred to in that article relating to a person previously identified as potentially having links to a threat, may be individually authorised. Where there are substantial grounds for believing that one or more persons belonging to the circle of the person to whom the authorisation relates are capable of providing information in respect of the purpose for which the authorisation was granted, authorisation may also be granted individually for each of those persons.  
I bis.      The maximum number of authorisations issued under this article in force at the same time shall be determined by the Prime Minister following consultation of the Commission for the Oversight of Intelligence Techniques. The decision establishing that quota and how it is to be allocated between the ministers referred to in the first paragraph of Article L. 821-2, together with the number of interception authorisations issued, shall be forwarded to the Commission.  
…’  
43      Article L. 851-3 of the CSI provides:  
‘I.      Under the conditions laid down in Chapter I of Title II of this Book, and for the sole purpose of preventing terrorism, the operators and persons referred to in Article L. 851-1 may be required to implement on their networks automated data processing practices designed, within the parameters laid down in the authorisation, to detect links that might constitute a terrorist threat.  
Such automated processing shall exclusively use the information or documents referred to in Article L. 851-1 and shall not collect any data other than data meeting the design parameters or allow the identification of the persons to whom the information or documents relate.  
In accordance with the principle of proportionality, the authorisation of the Prime Minister shall specify the technical scope of the implementation of those processing practices.  
II.      The Commission for the Oversight of Intelligence Techniques shall issue an opinion on the application for authorisation for automated processing and the chosen detection parameters. It shall have permanent, complete and direct access to those processing practices and to the information and data collected. It shall be informed of any changes to the processing practices and parameters and may issue recommendations.  
The first authorisation for the implementation of automated processing practices provided for in point I of this article shall be issued for a period of two months. The authorisation shall be renewable under the conditions on duration laid down in Chapter I of Title II of this Book. The application for renewal shall include a record of the number of identifiers flagged by the automated processing and an analysis of the relevance of that flagging.  
III.      The conditions laid down in Article L. 871-6 are applicable to the physical operations performed by the operators and persons referred to in Article L. 851-1 for the purpose of implementing such processing.  
IV.      Where the processing practices mentioned in point I of this article detect data likely to point to the existence of a terrorist threat, the Prime Minister or one of the persons delegated by him or her may – following consultation of the Commission for the Oversight of Intelligence Techniques under the conditions laid down in Chapter I of Title II of this Book – authorise the identification of the person or persons concerned and the collection of the related data. The data shall be used within 60 days of collection and shall be destroyed upon expiry of that period, unless there are substantial grounds confirming the existence of a terrorist threat associated with one or more of the persons concerned.  
…’  
44      Article L. 851-4 of the CSI reads as follows:  
‘Under the conditions laid down in Chapter I of Title II of this Book, technical data relating to the location of the terminal equipment used, as mentioned in Article L. 851-1, may be collected upon request from the network and transmitted in real time by the operators to a department reporting to the Prime Minister.’  
45      Article R. 851-5 of the CSI, which appears in the regulatory part of that code, provides:  
‘I.      The information or documents referred to in Article L. 851-1 are – excluding the content of the correspondence or the information consulted – as follows:  
1.      Those listed in Articles R. 10-13 and R. 10-14 of the [CPCE] and in Article 1 of Decree [No 2011-219];  
2.      Technical data other than the data mentioned in point 1:  
(a)      enabling terminal equipment to be located;  
(b)      relating to access by terminal equipment to online public communication networks or services;  
(c)      relating to the conveyance of electronic communications by networks;  
(d)      relating to the identification and authentication of a user, a connection, a network or an online public communication service;  
(e)      relating to the characteristics of terminal equipment and the configuration data of their software.  
II.      Only the information and documents referred to in point I(1) may be collected pursuant to Article L. 851-1. Such collection shall take place in non-real time.  
The information listed in point I(2) may be collected only pursuant to Articles L. 851-2 and L. 851-3 under the conditions and within the limits laid down in those articles and subject to the application of Article R. 851-9.’  
   
The CPCE  
46      Article L. 34-1 of the CPCE states:  
‘I.      This article shall apply to the processing of personal data in the course of the provision to the public of electronic communications services; it shall apply in particular to networks that support data collection and identification devices.  
II.      Electronic communications operators, in particular persons whose business is to provide access to online public communication services, shall erase or render anonymous any data relating to traffic, subject to the provisions contained in points III, IV, V and VI.  
Persons who provide electronic communications services to the public shall, with due regard for the provisions contained in the preceding paragraph, establish internal procedures for responding to requests from the competent authorities.  
Persons who, as a principal or ancillary business activity, provide to the public a connection allowing online communication via access to the network shall, including where this is offered free of charge, be subject to compliance with the provisions applicable to electronic communications operators under this article.  
III.      For the purposes of investigating, detecting and prosecuting criminal offences or a failure to fulfil an obligation laid down in Article L. 336-3 of the code de la propriété intellectuelle (Intellectual Property Code) or for the purposes of preventing breaches of automated data processing systems as provided for and punishable under Articles 323-1 to 323-3-1 of the Code pénal (Criminal Code), and for the sole purpose of making information available, as necessary, to the judicial authority or high authority mentioned in Article L. 331-12 of the Intellectual Property Code or to the national authority for the security of information systems mentioned in Article L. 2321-1 of the code de la défense (Defence Code), operations designed to erase or render anonymous certain categories of technical data may be deferred for a maximum period of one year. A decree adopted in the Conseil d’État (Council of State, France) following consultation of the Data Protection Authority shall, within the limits laid down in point VI, determine the categories of data involved and the period for which they are to be retained, depending on the business of the operators, the nature of the communications and the methods of offsetting any identifiable and specific additional costs associated with the services provided for these purposes by operators at the request of the State.  
…  
VI.      Data retained and processed under the conditions set out in points III, IV and V shall relate exclusively to the identification of persons using the services provided by operators, the technical characteristics of the communications provided by the latter and the location of terminal equipment.  
Under no circumstance may such data relate to the content of the correspondence or the information consulted, in any form whatsoever, as part of those communications.  
The retention and processing of such data shall be effected with due regard for the provisions of loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés (Law No 78-17 of 6 January 1978 on information technology, files and freedoms).  
Operators shall take any measures necessary to prevent such data from being used for purposes other than those provided for in this article.’  
47      Article R. 10-13 of the CPCE reads as follows:  
‘I.      Pursuant to point III of Article L. 34-1, electronic communications operators shall retain the following data for the purposes of investigating, detecting and prosecuting criminal offences:  
(a)      Information identifying the user;  
(b)      Data relating to the communications terminal equipment used;  
(c)      The technical characteristics and date, time and duration of each communication;  
(d)      Data relating to the additional services requested or used and the providers of those services;  
(e)      Data identifying the addressee or addressees of the communication.  
II.      In the case of telephony activities, the operator shall retain the data referred to in point II and, additionally, data enabling the origin and location of the communication to be identified.  
III.      The data referred to in this article shall be retained for one year from the date of registration.  
IV.      Identifiable and specific additional costs borne by operators which have been ordered by judicial authorities to provide data falling within the categories mentioned in this article shall be offset in accordance with the methods laid down in Article R. 213-1 of the code de procédure pénale (Code of Criminal Procedure).’  
48      Article R. 10-14 of the CPCE provides:  
‘I.      Pursuant to point IV of Article L. 34-1, electronic communications operators are authorised to retain technical data identifying the user and the data mentioned in Article R. 10-13(I)(b), (c) and (d) for the purposes of their billing and payment operations.  
II.      In the case of telephony activities, operators may retain, in addition to the data mentioned in point I, technical data relating to the location of the communication and the identification of the addressee or addressees of the communication and data for billing purposes.  
III.      The data mentioned in points I and II of this article may be retained only if it is necessary for billing purposes and for the payment of services rendered. Its retention shall be limited to the time strictly necessary for that purpose and shall not exceed one year.  
IV.      Operators may retain the following data for a period not exceeding three months to ensure the security of networks and facilities:  
(a)      Data identifying the origin of the communication;  
(b)      The technical characteristics and date, time and duration of each communication;  
(c)      Technical data identifying the addressee or addressees of the communication;  
(d)      Data relating to the additional services requested or used and the providers of those services.’  
   
Loi n° 2004  
-  
575 du 21 juin 2004 pour la confiance dans l’économie numérique (Law No 2004  
-  
575 of 21 June 2004 to promote trust in the digital economy)  
49      Article 6 of Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique (Law No 2004-575 of 21 June 2004 to promote trust in the digital economy) (JORF of 22 June 2004, p. 11168; ‘the LCEN’) provides:  
‘I.      1. Persons whose business is to provide access to online public communication services shall inform their subscribers of the existence of technical tools enabling access to some services to be restricted or for a selection of those services to be made and shall offer them at least one of those tools.  
…  
2.      Natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services, may not incur any civil liability for the activities or information stored at the request of a recipient of those services if they had no actual knowledge of either the unlawful nature of the activities or information in question or of the facts and circumstances pointing to their unlawful nature, or if, as soon as they became aware of that unlawful nature, they acted expeditiously to remove the data at issue or block access to them.  
…  
II.      The persons referred to in point I(1) and (2) shall keep and retain the data in such a way as to make it possible to identify anyone who has assisted in the creation of all or part of the content of the services of which they are the providers.  
They shall provide persons who publish an online public communication service with technical tools enabling them to satisfy the identification conditions laid down in point III.  
A judicial authority may require the service providers mentioned in point I(1) and (2) to communicate the data referred to in the first paragraph.  
The provisions of Articles 226-17, 226-21 and 226-22 of the Criminal Code shall apply to the processing of that data.  
A decree adopted in the Conseil d’État (Council of State, France) following consultation of the Data Protection Authority shall define the data referred to in the first paragraph and determine the period for which, and the methods by which, that data is to be retained.  
…’  
   
Decree No 2011  
-  
219  
50      Chapter I of Decree No 2011-219, adopted on the basis of the last paragraph of Article 6(II) of the LCEN, contains Articles 1 to 4 of that decree.  
51      Article 1 of Decree No 2011-219 provides:  
‘The following data is the data referred to in Article 6(II) of the [LCEN], which persons are required to retain under that provision:  
1.      For the persons referred to in point I(1) of that article and for each connection of their subscribers:  
(a)      The connection identifier;  
(b)      The identifier assigned by those persons to the subscriber;  
(c)      The identifier of the terminal used for the connection when they have access to it;  
(d)      The date and time of the start and end of the connection;  
(e)      The characteristics of the subscriber’s line.  
2.      For the persons referred to in point I(2) of that article and for each creation operation:  
(a)      The identifier of the connection giving rise to the communication;  
(b)      The identifier assigned by the information system to the content forming the subject of the operation;  
(c)      The types of protocols used to connect to the service and transfer the content;  
(d)      The nature of the operation;  
(e)      The date and time of the operation;  
(f)      The identifier used by the author of the operation where provided by the author.  
3.      For the persons referred to in point I(1) and (2) of that article, the information provided by a user when signing up to a contract or creating an account:  
(a)      The identifier of the connection at the time when the account was created;  
(b)      The first name and surname or business name;  
(c)      The associated postal addresses;  
(d)      The pseudonyms used;  
(e)      The associated email or account addresses;  
(f)      The telephone numbers;  
(g)      The updated password and the data for verifying or changing it.  
4.      For the persons referred to in point I(1) and (2) of that article, where the signing up to the contract or the account is subject to payment, the following information relating to the payment, for each payment operation:  
(a)      The type of payment used;  
(b)      The payment reference;  
(c)      The amount;  
(d)      The date and time of the transaction.  
The data mentioned in points 3 and 4 shall be retained only to the extent that the persons ordinarily collect such data.’  
52      Article 2 of that decree reads as follows:  
‘Contributing to the creation of content involves the following operations:  
(a)      Initial content creation;  
(b)      Changes to content and content-related data;  
(c)      Content erasure.’  
53      Article 3 of that decree provides:  
‘The data referred to in Article 1 shall be retained for one year from the date of:  
(a)      creation of the content, for each operation contributing to the creation of content as defined in Article 2, as regards the data mentioned in points 1 and 2;  
(b)      termination of the contract or closure of the account, as regards the data mentioned in point 3;  
(c)      issue of the bill or the payment operation, for each bill or payment operation, as regards the data mentioned in point 4.’  
   
Belgian law  
54      The Law of 29 May 2016 amended, in particular, the loi du 13 juin 2005 relative aux communications électroniques (Law of 13 June 2005 on electronic communications) (  
Moniteur belge  
 of 20 June 2005, p. 28070; ‘the Law of 13 June 2005’), the code d’instruction criminelle (Code of Criminal Procedure) and the loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Basic Law of 30 November 1998 on the intelligence and security services) (  
Moniteur belge  
 of 18 December 1998, p. 40312; ‘the Law of 30 November 1998’).  
55      Article 126 of the Law of 13 June 2005, as amended by the Law of 29 May 2016, provides:  
‘1.      Without prejudice to the Loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel (Law of 8 December 1992 on the protection of privacy with respect to the processing of personal data), providers to the public of telephony services, including via the Internet, Internet access and Internet-based email, operators providing public electronic communications networks and operators providing any of those services shall retain the data referred to in paragraph 3 where that data is generated or processed by them in the course of providing the communications services concerned.  
This article shall not concern the content of communications.  
The obligation to retain the data referred to in paragraph 3 shall also apply to unsuccessful call attempts, provided that that data is, in the course of providing the communications services concerned:  
(1)      generated or processed by operators of publicly available electronic communications services or of a public electronic communications network, so far as concerns telephony data, or  
(2)      logged by those providers, so far as concerns Internet data.  
2.      Data retained under this article may be obtained, by simple request, from the providers and operators referred to in the first subparagraph of paragraph 1, for the purposes and under the conditions listed below, only by the following authorities:  
(1)      judicial authorities, with a view to the investigation, detection and prosecution of offences, in order to execute the measures referred to in Articles 46bis and 88bis of the Code of Criminal Procedure and under the conditions laid down in those articles;  
(2)      under the conditions laid down in this law, intelligence and security services, in order to carry out intelligence missions employing the data-gathering methods referred to in Articles 16/2, 18/7 and 18/8 of the Basic Law of 30 November 1998 on the intelligence and security services;  
(3)      any judicial police officer attached to the [Institut belge des services postaux et des télécommunications (Belgian Institute for Postal Services and Telecommunications)], with a view to the investigation, detection and prosecution of offences contrary to Articles 114 and 124 and this article;  
(4)      emergency services providing on-site assistance, in the case where, after having received an emergency call, they cannot obtain from the provider or operator concerned the data identifying the person having made the emergency call using the database referred to in the third subparagraph of Article 107(2), or obtain incomplete or incorrect data. Only the data identifying the caller may be requested and the request must be made no later than 24 hours after the call;  
(5)      any judicial police officer attached to the Missing Persons Unit of the Federal Police, in the course of his or her task of providing assistance to persons in danger, searching for persons whose disappearance is a cause for concern and in cases where there are serious presumptions or indications that the physical well-being of the missing person is in imminent danger. Only the data referred to in the first and second subparagraphs of paragraph 3, relating to the missing person, and retained during the 48 hours prior to the data request, may be requested from the operator or provider concerned via a police service designated by the King;  
(6)      the Telecommunications Ombudsman, with a view to identifying a person who has misused an electronic communications network or service, in accordance with the conditions laid down in Article 43bis(3)(7) of the loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (Law of 21 March 1991 on the reform of certain public commercial undertakings). Only the identification data may be requested.  
The providers and operators referred to in the first subparagraph of paragraph 1 shall ensure that the data referred to in paragraph 3 are accessible without restriction from Belgium and that that data and any other necessary information concerning that data may be transmitted without delay and only to the authorities referred to in this paragraph.  
Without prejudice to other legal provisions, the providers and operators referred to in the first subparagraph of paragraph 1 may not use the data retained under paragraph 3 for any other purposes.  
3.      Data that can be used to identify the user or subscriber and the means of communication, other than the data specifically provided for in the second and third subparagraphs, shall be retained for 12 months as from the date on which communication was last able to be made using the service employed.  
Data relating to the terminal devices’ access and connection to the network and the service, and to the location of those devices, including the network termination point, shall be retained for 12 months as from the date of the communication.  
Communication data other than content, including the origin and destination thereof, shall be retained for 12 months as from the date of the communication.  
The King shall, by decree deliberated in the Council of Ministers and on a proposal from the Minister for Justice and the Minister [with responsibility for matters relating to electronic communications], and after obtaining the opinion of the Committee for the Protection of Privacy and the Institute, determine the data to be retained by category type as referred to in the first to third subparagraphs and the requirements which that data must satisfy.  
…’  
   
The disputes in the main proceedings and the questions referred for a preliminary ruling  
   
Case C  
-  
511/18  
56      By applications lodged on 30 November 2015 and 16 March 2016, joined in the main proceedings, La Quadrature du Net, French Data Network, the Fédération des fournisseurs d’accès à Internet associatifs and Igwan.net brought actions before the Conseil d’État (Council of State, France) for the annulment of Decrees No 2015-1185, No 2015-1211, No 2015-1639 and No 2016-67, on the ground, inter alia, that they infringe the French Constitution, the European Convention for the Protection of Human Rights and Fundamental Freedoms (‘the ECHR’) and Directives 2000/31 and 2002/58, read in the light of Articles 7, 8 and 47 of the Charter.  
57      As regards, in particular, the pleas alleging infringement of Directive 2000/31, the referring court states that the provisions of Article L. 851-3 of the CSI require electronic communications operators and technical service providers to ‘implement on their networks automated data processing practices designed, within the parameters laid down in the authorisation, to detect links that might constitute a terrorist threat’. That technique is intended only to facilitate the collection, for a limited period and from all of the connection data processed by those operators and service providers, of such data as might be related to a serious offence of this kind. In those circumstances, those provisions, which do not impose a general obligation of active surveillance, do not, in the view of the referring court, infringe Article 15 of Directive 2000/31.  
58      As regards the pleas alleging infringement of Directive 2002/58, the referring court considers that it follows, inter alia, from the provisions of that directive and from the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970; ‘  
Tele2  
’), that national provisions imposing obligations on providers of electronic communications services, such as the general and indiscriminate retention of the traffic and location data of their users and subscribers, for the purposes stated in Article 15(1) of that directive, which include safeguarding national security, defence and public security, fall within the scope of that directive since those rules govern the activity of those providers. That also applies to rules governing access to and use of data by national authorities.  
59      The referring court concludes from this that both the obligation to retain data resulting from Article L. 851-1 of the CSI and the access of the administrative authorities to that data, including real-time access, provided for in Articles L. 851-1, L. 851-2 and L. 851-4 of that code, fall within the scope of Directive 2002/58. The same is true, according to that court, of the provisions of Article L. 851-3 of the CSI, which, although they do not impose a general retention obligation on the operators concerned, do however require them to implement automated processing on their networks that is intended to detect links that might constitute a terrorist threat.  
60      On the other hand, the referring court takes the view that the scope of Directive 2002/58 does not extend to the provisions of the CSI referred to in the applications for annulment which relate to intelligence gathering techniques applied directly by the State, but do not regulate the activities of providers of electronic communications services by imposing specific obligations on them. Accordingly, those provisions cannot be regarded as implementing EU law, with the result that the pleas alleging that they infringe Directive 2002/58 cannot validly be relied on.  
61      Thus, with a view to settling the disputes concerning the lawfulness of Decrees No 2015-1185, No 2015-1211, No 2015-1639 and No 2016-67 in the light of Directive 2002/58, in so far as they were adopted to implement Articles L. 851-1 to L. 851-4 of the CSI, three questions on the interpretation of EU law arise.  
62      As regards the interpretation of Article 15(1) of Directive 2002/58, the referring court is uncertain, in the first place, whether a general and indiscriminate retention obligation, imposed on providers of electronic communications services on the basis of Articles L. 851-1 and R. 851-5 of the CSI, is to be regarded in the light, inter alia, of the safeguards and checks to which the access of the administrative authorities to and the use of connection data are subject, as interference justified by the right to security guaranteed in Article 6 of the Charter and by the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 TEU.  
63      As regards, in the second place, the other obligations which may be imposed on providers of electronic communications services, the referring court states that the provisions of Article L. 851-2 of the CSI permit, for the sole purpose of preventing terrorism, the collection of the information or documents referred to in Article L. 851-1 of that code from the same persons. Such collection, in relation solely to one or more individuals previously identified as potentially having links to a terrorist threat, is to be carried out in real time. The same is true of the provisions of Article L. 851-4, which authorise the real-time transmission by operators exclusively of technical data relating to the location of terminal equipment. Those techniques regulate the real-time access of the administrative authorities to data retained under the CPCE and the LCEN for various purposes and by various means, without, however, imposing on the providers concerned any additional retention requirement over and above what is necessary for the billing and provision of their services. In the same vein, nor do the provisions of Article L. 851-3 of the CSI, which require service providers to implement on their networks an automated system for the analysis of connections, entail general and indiscriminate retention.  
64      The referring court considers that both general and indiscriminate retention and real-time access to connection data are of unparalleled operational usefulness, against a background of serious and persistent threats to national security, in particular the terrorist threat. General and indiscriminate retention allows the intelligence services to obtain access to communications data before the reasons for believing that the person concerned poses a threat to public security, defence or State security are identified. In addition, real-time access to connection data makes it possible to monitor, with a high level of responsiveness, the conduct of individuals who may pose an immediate threat to public order.  
65      Furthermore, the technique provided for in Article L. 851-3 of the CSI makes it possible to detect, on the basis of criteria specifically defined for that purpose, those individuals whose conduct may, in view of their methods of communication, constitute a terrorist threat.  
66      In the third place, as regards access by the competent authorities to retained data, the referring court is unsure whether Directive 2002/58, read in the light of the Charter, is to be interpreted as meaning that it is a prerequisite for the lawfulness of the procedures for the collection of connection data that the data subjects are informed whenever their being so informed is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or whether such procedures may be regarded as lawful taking into account all the other procedural safeguards provided for in national law where those safeguards ensure that the right to a remedy is effective.  
67      As regards those other procedural safeguards, the referring court states in particular that any person wishing to verify that no intelligence techniques have been unlawfully implemented against him or her may bring the matter before a specialist panel of the Conseil d’État (Council of State, France), which is responsible for determining – in the light of the information communicated to it outside   
inter partes  
 proceedings – whether the applicant has been the subject of an intelligence technique and whether that technique was implemented in accordance with Book VIII of the CSI. The powers conferred on that panel to investigate applications ensure that the judicial review conducted by it is effective. Thus, it has jurisdiction to investigate applications, to raise of its own motion any illegalities it may find and to order the authorities to take all appropriate measures to remedy the illegalities found. In addition, it is for the Commission for the Oversight of Intelligence Techniques to check that intelligence gathering techniques are implemented, on national territory, in accordance with the requirements flowing from the CSI. Thus, the fact that the legislative provisions at issue in the main proceedings do not provide for the notification to the persons concerned of the surveillance measures applied to them does not, in itself, constitute excessive interference with the right to respect for private life.  
68      It is on that basis that the Conseil d’État (Council of State, France) decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Is the general and indiscriminate retention obligation imposed on providers on the basis of the implementing provisions of Article 15(1) of [Directive 2002/58] to be regarded, against a background of serious and persistent threats to national security, and in particular the terrorist threat, as interference justified by the right to security guaranteed in Article 6 of the [Charter] and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 [TEU]?  
(2)      Is [Directive 2002/58], read in the light of the [Charter], to be interpreted as authorising legislative measures, such as the measures for the real-time collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data?  
(3)      Is [Directive 2002/58], read in the light of the [Charter], to be interpreted as meaning that it is a prerequisite for the lawfulness of the procedures for the collection of connection data that the data subjects are informed whenever their being so informed is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or may such procedures be regarded as lawful taking into account all the other existing procedural safeguards where those safeguards ensure that the right to a remedy is effective?’  
   
Case C  
-  
512/18  
69      By application lodged on 1 September 2015, French Data Network, La Quadrature du Net and the Fédération des fournisseurs d’accès à Internet associatifs brought an action before the Conseil d’État (Council of State, France) for the annulment of the implied rejection decision arising from the Prime Minister’s failure to reply to their application for the repeal of Article R. 10-13 of the CPCE and Decree No 2011-219, on the ground, inter alia, that those legislative texts infringe Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 of the Charter. Privacy International and the Center for Democracy and Technology were granted leave to intervene in the main proceedings.  
70      As regards Article R. 10-13 of the CPCE and the obligation of general and indiscriminate retention of communications data laid down therein, the referring court, which raises similar considerations to those in Case C-511/18, observes that such retention allows a judicial authority to access data relating to communications made by an individual before being suspected of having committed a criminal offence, with the result that such retention is of unparalleled usefulness for the investigation, detection and prosecution of criminal offences.  
71      As regards Decree No 2011-219, the referring court considers that Article 6(II) of the LCEN, which imposes an obligation to hold and retain only data relating to the creation of content, does not fall within the scope of Directive 2002/58 since that directive’s scope is limited, in accordance with Article 3(1) thereof, to the provision of publicly available electronic communications services in public communications networks in the European Union. On the other hand, that national provision does fall within the scope of Directive 2000/31.  
72      The referring court considers, however, that it follows from Article 15(1) and (2) of Directive 2000/31 that the directive does not establish a prohibition in principle on retaining data relating to the creation of content, from which derogation would be possible only by way of exception. Thus, the question arises whether Articles 12, 14 and 15 of Directive 2000/31, read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the Charter, are to be interpreted as allowing a Member State to introduce national legislation, such as Article 6(II) of the LCEN, which requires the persons concerned to retain data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that a judicial authority may, where appropriate, require the communication of that data with a view to ensuring compliance with the rules on civil and criminal liability.  
73      It is on that basis that the Conseil d’État (Council of State, France) decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Is the general and indiscriminate retention obligation imposed on providers on the basis of the implementing provisions of Article 15(1) of [Directive 2002/58] to be regarded, inter alia in the light of the safeguards and checks to which the collection and use of such connection data are then subject, as interference justified by the right to security guaranteed in Article 6 of the [Charter] and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 [TEU]?  
(2)      Are the provisions of [Directive 2000/31], read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the [Charter], to be interpreted as allowing a State to introduce national legislation requiring the persons, whose activity consists in offering access to online public communications services and the natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services, to retain the data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that a judicial authority may, where appropriate, require the communication of that data with a view to ensuring compliance with the rules on civil and criminal liability?’  
   
Case C  
-  
520/18  
74      By applications lodged on 10, 16, 17 and 18 January 2017, joined in the main proceedings, the Ordre des barreaux francophones et germanophone, the Académie Fiscale ASBL and UA, the Liga voor Mensenrechten ASBL, the Ligue des Droits de l’Homme ASBL, and VZ, WY and XX brought actions before the Cour constitutionnelle (Constitutional Court, Belgium) for the annulment of the Law of 29 May 2016, on the ground that it infringes Articles 10 and 11 of the Belgian Constitution, read in conjunction with Articles 5, 6 to 11, 14, 15, 17 and 18 of the ECHR, Articles 7, 8, 11 and 47 and Article 52(1) of the Charter, Article 17 of the International Covenant on Civil and Political Rights, which was adopted by the United Nations General Assembly on 16 December 1966 and entered into force on 23 March 1976, the general principles of legal certainty, proportionality and self-determination in relation to information and Article 5(4) TEU.  
75      In support of their actions, the applicants in the main proceedings submit, in essence, that the Law of 29 May 2016 is unlawful because, among other things, it goes beyond what is strictly necessary and does not lay down adequate guarantees of protection. In particular, neither its provisions relating to the retention of data nor those governing access by the authorities to retained data satisfy the requirements deriving from the judgments of 8 April 2014,   
Digital Rights Ireland and Others  
 (C-293/12 and C-594/12, EU:C:2014:238; ‘  
Digital Rights  
’) and of 21 December 2016,   
Tele2  
 (C-203/15 and C-698/15, EU:C:2016:970). They contend that those provisions entail a risk that personality profiles will be compiled, which may be misused by the competent authorities, and that they do not establish an appropriate level of security and protection for the retained data. Lastly, that law covers persons who are bound by professional secrecy and persons who are under a duty of confidentiality, and applies to personal communication data that is sensitive, without including specific safeguards to protect such data.  
76      The referring court observes that the data which must be retained by providers of telephony services, including via the Internet, Internet access and Internet-based email and by operators providing public electronic communications networks, under the Law of 29 May 2016, is identical to that listed in Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), without any distinction being made as regards the persons concerned or on the basis of the objective pursued. As regards the latter point, the referring court states that the objective pursued by the legislature by means of that law is not only to combat terrorism and child pornography, but also to enable the use of the retained data in a wide variety of situations in the context of criminal investigations. The referring court also notes that it is apparent from the explanatory memorandum for that law that the national legislature considered it impossible, in the light of the objective pursued, to impose a targeted and selective obligation to retain data, and that it chose to apply strict guarantees to the general and indiscriminate retention obligation, both as regards the data retained and access to that data, in order to keep interference with the right to respect for private life to a minimum.  
77      The referring court also states that subparagraphs 1 and 2 of Article 126(2) of the Law of 13 June 2005, as amended by the Law of 29 May 2016, lay down the conditions under which, respectively, judicial authorities and the intelligence and security services may obtain access to retained data, and consequently the review of the lawfulness of that law in the light of the requirements of EU law should be deferred until the Court has adjudicated on two preliminary ruling procedures pending before it concerning such access.  
78      Lastly, the referring court states that the Law of 29 May 2016 seeks to ensure an effective criminal investigation and effective penalties in cases involving the sexual abuse of minors and to make it possible to identify the perpetrator of such an offence, even where electronic communications systems are used. In the proceedings before it, attention was drawn in that respect to the positive obligations under Articles 3 and 8 of the ECHR. Those obligations may also arise under the corresponding provisions of the Charter, which may have consequences for the interpretation of Article 15(1) of Directive 2002/58.  
79      It is on that basis that the Cour constitutionnelle (Constitutional Court, Belgium) decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Must Article 15(1) of [Directive 2002/58], read in conjunction with the right to security, guaranteed by Article 6 of the [Charter], and the right to respect for personal data, as guaranteed by Articles 7, 8 and 52(1) of the [Charter], be interpreted as precluding national legislation such as that at issue, which lays down a general obligation for operators and providers of electronic communications services to retain the traffic and location data within the meaning of [Directive 2002/58], generated or processed by them in the context of the supply of those services, national legislation whose objective is not only the investigation, detection and prosecution of serious criminal offences but also the safeguarding of national security, the defence of the territory and of public security, the investigation, detection and prosecution of offences other than serious crime or the prevention of the prohibited use of electronic communication systems, or the attainment of another objective identified by Article 23(1) of [Regulation 2016/679] and which, furthermore, is subject to specific safeguards in that legislation in terms of data retention and access to that data?  
(2)      Must Article 15(1) of [Directive 2002/58], in conjunction with Articles 4, 7, 8, 11 and 52(1) of the [Charter], be interpreted as precluding national legislation such as that at issue, which lays down a general obligation for operators and providers of electronic communications services to retain the traffic and location data within the meaning of [Directive 2002/58], generated or processed by them in the context of the supply of those services, if the object of that legislation is, in particular, to comply with the positive obligations borne by the authority under Articles 4 and [7] of the Charter, consisting in the provision of a legal framework which allows the effective criminal investigation and the effective punishment of sexual abuse of minors and which permits the effective identification of the perpetrator of the offence, even where electronic communications systems are used?  
(3)      If, on the basis of the answer to the first or the second question, the Cour constitutionnelle (Constitutional Court, Belgium) should conclude that the contested law fails to fulfil one or more obligations arising under the provisions referred to in these questions, might it maintain on a temporary basis the effects of [the Law of 29 May 2016] in order to avoid legal uncertainty and to enable the data previously collected and retained to continue to be used for the objectives pursued by the law?’  
   
Procedure before the Court  
80      By decision of the President of the Court of 25 September 2018, Cases C-511/18 and C-512/18 were joined for the purposes of the written and oral parts of the procedure and the judgment. Case C-520/18 was joined to those cases by decision of the President of the Court of 9 July 2020 for the purposes of the judgment.  
   
Consideration of the questions referred  
   
Question  
   
1 in Cases C  
-  
511/18 and C  
-  
512/18 and questions  
   
1 and 2 in Case C  
-  
520/18  
81      By question 1 in Cases C-511/18 and C-512/18 and questions 1 and 2 in Case C-520/18, which should be considered together, the referring courts essentially ask whether Article 15(1) of Directive 2002/58 must be interpreted as precluding national legislation which imposes on providers of electronic communications services, for the purposes set out in Article 15(1), an obligation requiring the general and indiscriminate retention of traffic and location data.  
   
Preliminary remarks  
82      It is apparent from the documents available to the Court that the legislation at issue in the main proceedings covers all electronic communications systems and applies to all users of such systems, without distinction or exception. Furthermore, the data which must be retained by providers of electronic communications services under that legislation is, in particular, the data necessary for locating the source of a communication and its destination, for determining the date, time, duration and type of communication, for identifying the communications equipment used, and for locating the terminal equipment and communications, data which comprises, inter alia, the name and address of the user, the telephone numbers of the caller and the person called, and the IP address for Internet services. By contrast, that data does not cover the content of the communications concerned.  
83      Thus, the data which must, under the national legislation at issue in the main proceedings, be retained for a period of one year makes it possible, inter alia, to identify the person with whom the user of an electronic communications system has communicated and by what means, to determine the date, time and duration of the communications and Internet connections and the place from which those communications and connections took place, and to ascertain the location of the terminal equipment without any communication necessarily having been transmitted. In addition, that data enables the frequency of a user’s communications with certain persons over a given period of time to be established. Last, as regards the national legislation at issue in Cases C-511/18 and C-512/18, it appears that that legislation, in so far as it also covers data relating to the conveyance of electronic communications by networks, also enables the nature of the information consulted online to be identified.  
84      As for the aims pursued, it should be noted that the legislation at issue in Cases C-511/18 and C-512/18 pursues, among other aims, the investigation, detection and prosecution of criminal offences in general; national independence, territorial integrity and national defence; major foreign policy interests; the implementation of France’s European and international commitments; France’s major economic, industrial and scientific interests; and the prevention of terrorism, attacks against the republican nature of the institutions and collective violence liable to cause serious disruption to the maintenance of law and order. The objectives of the legislation at issue in Case C-520/18 are, inter alia, the investigation, detection and prosecution of criminal offences and the safeguarding of national security, the defence of the territory and public security.  
85      The referring courts are uncertain, in particular, as to the possible impact of the right to security enshrined in Article 6 of the Charter on the interpretation of Article 15(1) of Directive 2002/58. Similarly, they ask whether the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter entailed by the retention of data provided for in the legislation at issue in the main proceedings may, in the light of the existence of rules restricting national authorities’ access to retained data, be regarded as justified. In addition, according to the Conseil d’État (Council of State, France), since that question arises in a context characterised by serious and persistent threats to national security, it should also be assessed in the light of Article 4(2) TEU. The Cour constitutionnelle (Constitutional Court, Belgium), for its part, points out that the national legislation at issue in Case C-520/18 also implements positive obligations flowing from Articles 4 and 7 of the Charter, consisting in the establishment of a legal framework for the effective prevention and punishment of the sexual abuse of minors.  
86      While both the Conseil d’État (Council of State, France) and the Cour constitutionnelle (Constitutional Court, Belgium) start from the premiss that the respective national legislation at issue in the main proceedings, which governs the retention of traffic and location data and access to that data by national authorities for the purposes set out in Article 15(1) of Directive 2002/58, such as safeguarding national security, falls within the scope of that directive, a number of parties to the main proceedings and some of the Member States which submitted written observations to the Court disagree on that point, particularly concerning the interpretation of Article 1(3) of that directive. It is therefore necessary to examine, first of all, whether the legislation at issue falls within the scope of that directive.  
   
Scope of Directive 2002/58  
87      La Quadrature du Net, the Fédération des fournisseurs d’accès à Internet associatifs, Igwan.net, Privacy International and the Center for Democracy and Technology rely on the Court’s case-law on the scope of Directive 2002/58 to argue, in essence, that both the retention of data and access to retained data fall within that scope, whether that access takes place in non-real time or in real time. Indeed, they contend that since the objective of safeguarding national security is expressly mentioned in Article 15(1) of that directive, the pursuit of that objective does not render that directive inapplicable. In their view, Article 4(2) TEU, mentioned by the referring courts, does not affect that assessment.  
88      As regards the intelligence measures implemented directly by the competent French authorities, without regulating the activities of providers of electronic communications services by imposing specific obligations on them, the Center for Democracy and Technology observes that those measures necessarily fall within the scope of Directive 2002/58 and of the Charter, since they are exceptions to the principle of confidentiality guaranteed in Article 5 of that directive. Those measures must therefore comply with the requirements stemming from Article 15(1) of the directive.  
89      On the other hand, the Czech and Estonian Governments, Ireland, and the French, Cypriot, Hungarian, Polish, Swedish and United Kingdom Governments submit, in essence, that Directive 2002/58 does not apply to national legislation such as that at issue in the main proceedings, since the purpose of that legislation is to safeguard national security. The intelligence services’ activities, in so far as they relate to the maintenance of public order and to the safeguarding of internal security and territorial integrity, are part of the essential functions of the Member States and, consequently, are within their exclusive competence, as evidenced, in particular, by the third sentence of Article 4(2) TEU.  
90      Those governments and Ireland also refer to Article 1(3) of Directive 2002/58, which excludes from the scope of that directive, as the first indent of Article 3(2) of Directive 95/46 did in the past, activities concerning public security, defence and State security. They rely in that regard on the interpretation of the latter provision set out in the judgment of 30 May 2006,   
Parliament  
 v   
Council and Commission  
 (C-317/04 and C-318/04, EU:C:2006:346).  
91      In that regard, it should be stated that, under Article 1(1) thereof, Directive 2002/58 provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector.  
92      Article 1(3) of that directive excludes from its scope ‘activities of the State’ in specified fields, including activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters. The activities thus mentioned by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 32 and the case-law cited).  
93      In addition, Article 3 of Directive 2002/58 states that that directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices (‘electronic communications services’). Consequently, that directive must be regarded as regulating the activities of the providers of such services (judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 33 and the case-law cited).  
94      In that context, Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, ‘legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of [that directive]’ (judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 71).  
95      Article 15(1) of Directive 2002/58 necessarily presupposes that the national legislative measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met. Further, such measures regulate, for the purposes mentioned in that provision, the activity of providers of electronic communications services (judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 34 and the case-law cited).  
96      It is in the light of, inter alia, those considerations that the Court has held that Article 15(1) of Directive 2002/58, read in conjunction with Article 3 thereof, must be interpreted as meaning that the scope of that directive extends not only to a legislative measure that requires providers of electronic communications services to retain traffic and location data, but also to a legislative measure requiring them to grant the competent national authorities access to that data. Such legislative measures necessarily involve the processing, by those providers, of the data and cannot, to the extent that they regulate the activities of those providers, be regarded as activities characteristic of States, referred to in Article 1(3) of that directive (see, to that effect, judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraphs 35 and 37 and the case-law cited).  
97      In addition, having regard to the considerations set out in paragraph 95 above and the general scheme of Directive 2002/58, an interpretation of that directive under which the legislative measures referred to in Article 15(1) thereof were excluded from the scope of that directive because the objectives which such measures must pursue overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that same directive would deprive Article 15(1) thereof of any practical effect (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 72 and 73).  
98      The concept of ‘activities’ referred to in Article 1(3) of Directive 2002/58 cannot therefore, as was noted, in essence, by the Advocate General in point 75 of his Opinion in Joined Cases   
La Quadrature du Net and Others  
 (C-511/18 and C-512/18, EU:C:2020:6), be interpreted as covering the legislative measures referred to in Article 15(1) of that directive.  
99      Article 4(2) TEU, to which the governments listed in paragraph 89 of the present judgment have made reference, cannot invalidate that conclusion. Indeed, according to the Court’s settled case-law, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law (see, to that effect, judgments of 4 June 2013,   
ZZ  
, C-300/11, EU:C:2013:363, paragraph 38; of 20 March 2018,   
Commission  
 v   
Austria (State printing office)  
, C-187/16, EU:C:2018:194, paragraphs 75 and 76; and of 2 April 2020,   
Commission  
 v   
Poland, Hungary and Czech Republic (Temporary mechanism for the relocation of applicants for international protection)  
, C-715/17, C-718/17 and C-719/17, EU:C:2020:257, paragraphs 143 and 170).  
100    It is true that, in the judgment of 30 May 2006,   
Parliament  
 v   
Council and Commission  
 (C-317/04 and C-318/04, EU:C:2006:346, paragraphs 56 to 59), the Court held that the transfer of personal data by airlines to the public authorities of a third country for the purpose of preventing and combating terrorism and other serious crimes did not, pursuant to the first indent of Article 3(2) of Directive 95/46, fall within the scope of that directive, because that transfer fell within a framework established by the public authorities relating to public security.  
101    However, having regard to the considerations set out in paragraphs 93, 95 and 96 of the present judgment, that case-law cannot be transposed to the interpretation of Article 1(3) of Directive 2002/58. Indeed, as the Advocate General noted, in essence, in points 70 to 72 of his Opinion in Joined Cases   
La Quadrature du Net and Others  
 (C-511/18 and C-512/18, EU:C:2020:6), the first indent of Article 3(2) of Directive 95/46, to which that case-law relates, excluded, in a general way, from the scope of that directive ‘processing operations concerning public security, defence, [and] State security’, without drawing any distinction according to who was carrying out the data processing operation concerned. By contrast, in the context of interpreting Article 1(3) of Directive 2002/58, it is necessary to draw such a distinction. As is apparent from paragraphs 94 to 97 of the present judgment, all operations processing personal data carried out by providers of electronic communications services fall within the scope of that directive, including processing operations resulting from obligations imposed on those providers by the public authorities, although those processing operations could, where appropriate, on the contrary, fall within the scope of the exception laid down in the first indent of Article 3(2) of Directive 95/46, given the broader wording of that provision, which covers all processing operations concerning public security, defence, or State security, regardless of the person carrying out those operations.  
102    Furthermore, it should be noted that Directive 95/46, which was at issue in the case that gave rise to the judgment of 30 May 2006,   
Parliament   
v   
Council and Commission  
 (C-317/04 and C-318/04, EU:C:2006:346), has been, pursuant to Article 94(1) of Regulation 2016/679, repealed and replaced by that regulation with effect from 25 May 2018. Although that regulation states, in Article 2(2)(d) thereof, that it does not apply to processing operations carried out ‘by competent authorities’ for the purposes of, inter alia, the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security, it is apparent from Article 23(1)(d) and (h) of that regulation that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation. It follows that the above interpretation of Article 1(3), Article 3 and Article 15(1) of Directive 2002/58 is consistent with the definition of the scope of Regulation 2016/679, which is supplemented and specified by that directive.  
103    By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only, subject to the application of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89), with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR.  
104    It follows from the foregoing considerations that national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes of protecting national security and combating crime, such as the legislation at issue in the main proceedings, falls within the scope of Directive 2002/58.  
   
Interpretation of Article 15(1) of Directive 2002/58  
105    It should be noted, as a preliminary point, that it is settled case-law that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation (see, to that effect, judgment of 17 April 2018,   
Egenberger  
, C-414/16, EU:C:2018:257, paragraph 44).  
106    As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of Directive 2002/58 is to protect users of electronic communications services from risks for their personal data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, that directive seeks, as is stated in recital 2 thereof, to ensure that the rights set out in Articles 7 and 8 of the Charter are fully respected. In that regard, it is apparent from the Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM (2000) 385 final), which gave rise to Directive 2002/58, that the EU legislature sought to ‘ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used’.  
107    To that end, Article 5(1) of Directive 2002/58 enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires, inter alia, that, in principle, persons other than users be prohibited from storing, without those users’ consent, those communications and that data.  
108    As regards, in particular, the processing and storage of traffic data by providers of electronic communications services, it is apparent from Article 6 and recitals 22 and 26 of Directive 2002/58 that such processing is permitted only to the extent necessary and for the time necessary for the marketing and billing of services and the provision of value added services. Once that period has elapsed, the data that has been processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers has been obtained (judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 86 and the case-law cited).  
109    Thus, in adopting that directive, the EU legislature gave concrete expression to the rights enshrined in Articles 7 and 8 of the Charter, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise.  
110    However, Article 15(1) of Directive 2002/58 enables the Member States to introduce exceptions to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to, inter alia, in Articles 6 and 9 of that directive, where such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. To that end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on one of those grounds.  
111    That being said, the option to derogate from the rights and obligations laid down in Articles 5, 6 and 9 of Directive 2002/58 cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of that data, explicitly laid down in Article 5 of that directive, to become the rule (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 89 and 104).  
112    As regards the objectives that are capable of justifying a limitation of the rights and obligations laid down, in particular, in Articles 5, 6 and 9 of Directive 2002/58, the Court has previously held that the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives (see, to that effect, judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 52 and the case-law cited).  
113    In addition, it is apparent from the third sentence of Article 15(1) of Directive 2002/58 that the Member States are not permitted to adopt legislative measures to restrict the scope of the rights and obligations provided for in Articles 5, 6 and 9 of that directive unless they do so in accordance with the general principles of EU law, including the principle of proportionality, and with the fundamental rights guaranteed in the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making them available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (see, to that effect, judgments of 8 April 2014,   
Digital Rights  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 25 and 70, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 91and 92 and the case-law cited).  
114    Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that that fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 6 March 2001,   
Connolly  
 v   
Commission  
, C-274/99 P, EU:C:2001:127, paragraph 39, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 93 and the case-law cited).  
115    It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, on the one hand, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing that data, and, on the other, an interference with the fundamental rights to respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (see, to that effect, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126 and the case-law cited; see, by analogy, as regards Article 8 of the ECHR, ECtHR, 30 January 2020,   
Breyer v. Germany  
, CE:ECHR:2020:0130JUD005000112, § 81).  
116    Whether or not the retained data has been used subsequently is also irrelevant (see, by analogy, as regards Article 8 of the ECHR, ECtHR, 16 February 2000,   
Amann v. Switzerland  
, CE:ECHR:2000:0216JUD002779895, § 69, and 13 February 2020,   
Trajkovski and Chipovski v. North Macedonia  
, CE:ECHR:2020:0213JUD005320513, § 51), since access to such data is a separate interference with the fundamental rights referred to in the preceding paragraph, irrespective of the subsequent use made of it (see, to that effect, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126).  
117    That conclusion is all the more justified since traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (see, to that effect, judgments of 8 April 2014,   
Digital Rights  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 27, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 99).  
118    Therefore, first, the retention of traffic and location data for policing purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of electronic communications systems from exercising their freedom of expression, guaranteed in Article 11 of the Charter (see, to that effect, judgments of 8 April 2014,   
Digital Rights  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 28, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 101). Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistleblowers whose actions are protected by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ 2019 L 305, p. 17). Moreover, that deterrent effect is all the more serious given the quantity and breadth of data retained.  
119    Second, in view of the significant quantity of traffic and location data that may be continuously retained under a general and indiscriminate retention measure, as well as the sensitive nature of the information that may be gleaned from that data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access.  
120    That being said, in so far as Article 15(1) of Directive 2002/58 allows Member States to introduce the derogations referred to in paragraph 110 above, that provision reflects the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 172 and the case-law cited).  
121    Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.  
122    Thus, in order to interpret Article 15(1) of Directive 2002/58 in the light of the Charter, account must also be taken of the importance of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter and of the importance of the objectives of protecting national security and combating serious crime in contributing to the protection of the rights and freedoms of others.  
123    In that regard, Article 6 of the Charter, to which the Conseil d’État (Council of State, France) and the Cour constitutionnelle (Constitutional Court, Belgium) refer, lays down the right of every individual not only to liberty but also to security and guarantees rights corresponding to those guaranteed in Article 5 of the ECHR (see, to that effect, judgments of 15 February 2016,   
N.  
, C-601/15 PPU, EU:C:2016:84, paragraph 47; of 28 July 2016,   
JZ  
, C-294/16 PPU, EU:C:2016:610, paragraph 48; and of 19 September 2019,   
Rayonna prokuratura Lom  
, C-467/18, EU:C:2019:765, paragraph 42 and the case-law cited).  
124    In addition, it should be recalled that Article 52(3) of the Charter is intended to ensure the necessary consistency between the rights contained in the Charter and the corresponding rights guaranteed in the ECHR, without adversely affecting the autonomy of EU law and that of the Court of Justice of the European Union. Account must therefore be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold of protection (see, to that effect, judgments of 12 February 2019,   
TC  
, C-492/18 PPU, EU:C:2019:108, paragraph 57, and of 21 May 2019,   
Commission  
 v   
Hungary (Rights of usufruct over agricultural land)  
, C-235/17, EU:C:2019:432, paragraph 72 and the case-law cited).  
125    Article 5 of the ECHR, which enshrines the ‘right to liberty’ and the ‘right to security’, is intended, according to the case-law of the European Court of Human Rights, to ensure that individuals are protected from arbitrary or unjustified deprivations of liberty (see, to that effect, ECtHR, 18 March 2008,   
Ladent v. Poland  
, CE:ECHR:2008:0318JUD001103603, §§ 45 and 46; 29 March 2010,   
Medvedyev and Others v. France  
, CE:ECHR:2010:0329JUD000339403, §§ 76 and 77; and 13 December 2012,   
El-Masri v. ‘The former Yugoslav Republic of Macedonia’  
, CE:ECHR:2012:1213JUD003963009, § 239). However, since that provision applies to deprivations of liberty by a public authority, Article 6 of the Charter cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences.  
126    On the other hand, as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, mentioned by the Cour constitutionnelle (Constitutional Court, Belgium), it should be pointed out that positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life (see, to that effect, judgment of 18 June 2020,   
Commission  
 v   
Hungary (Transparency of associations)  
, C-78/18, EU:C:2020:476, paragraph 123 and the case-law cited of the European Court of Human Rights). Such obligations may also arise from Article 7, concerning the protection of an individual’s home and communications, and Articles 3 and 4, as regards the protection of an individual’s physical and mental integrity and the prohibition of torture and inhuman and degrading treatment.  
127    It is against the backdrop of those different positive obligations that the Court must strike a balance between the various interests and rights at issue.  
128    The European Court of Human Rights has held that the positive obligations flowing from Articles 3 and 8 of the ECHR, whose corresponding safeguards are set out in Articles 4 and 7 of the Charter, require, in particular, the adoption of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against the person through effective investigation and prosecution, that obligation being all the more important when a child’s physical and moral well-being is at risk. However, the measures to be taken by the competent authorities must fully respect due process and the other safeguards limiting the scope of criminal investigation powers, as well as other freedoms and rights. In particular, according to that court, a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected (ECtHR, 28 October 1998,   
Osman v. United Kingdom  
, CE:ECHR:1998:1028JUD002345294, §§ 115 and 116; 4 March 2004,   
M.C. v. Bulgaria  
, CE:ECHR:2003:1204JUD003927298, § 151; 24 June 2004,   
Von Hannover v. Germany  
, CE:ECHR:2004:0624JUD005932000, §§ 57 and 58; and 2 December 2008,   
K.U. v. Finland  
, CE:ECHR:2008:1202JUD000287202, §§ 46, 48 and 49).  
129    Concerning observance of the principle of proportionality, the first sentence of Article 15(1) of Directive 2002/58 provides that the Member States may adopt a measure derogating from the principle that communications and the related traffic data are to be confidential where such a measure is ‘necessary, appropriate and proportionate … within a democratic society’, in view of the objectives set out in that provision. Recital 11 of that directive specifies that a measure of that nature must be ‘strictly’ proportionate to the intended purpose.  
130    In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (see, to that effect, judgments of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 56; of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 76, 77 and 86; and of 8 April 2014,   
Digital Rights  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52; Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 140).  
131    Specifically, it follows from the Court’s case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness (see, to that effect, judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 55 and the case-law cited).  
132    In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake (see, to that effect, judgments of 8 April 2014,   
Digital Rights  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 117; Opinion 1/15 (  
EU-Canada   
PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 141).  
133    Thus, legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued (see, to that effect, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 191 and the case-law cited, and judgment of 3 October 2019,   
A and Others  
, C-70/18, EU:C:2019:823, paragraph 63).  
–         
Legislative measures providing for the preventive retention of traffic and location data for the purpose of safeguarding national security  
134    It should be observed that the objective of safeguarding national security, mentioned by the referring courts and the governments which submitted observations, has not yet been specifically examined by the Court in its judgments interpreting Directive 2002/58.  
135    In that regard, it should be noted, at the outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.  
136    The importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats such as those referred to in the preceding paragraph can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.  
137    Thus, in situations such as those described in paragraphs 135 and 136 of the present judgment, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat, as referred to in paragraphs 135 and 136 of the present judgment, to national security which is shown to be genuine and present or foreseeable. Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.  
138    The instruction for the preventive retention of data of all users of electronic communications systems must, however, be limited in time to what is strictly necessary. Although it is conceivable that an instruction requiring providers of electronic communications services to retain data may, owing to the ongoing nature of such a threat, be renewed, the duration of each instruction cannot exceed a foreseeable period of time. Moreover, such data retention must be subject to limitations and must be circumscribed by strict safeguards making it possible to protect effectively the personal data of the persons concerned against the risk of abuse. Thus, that retention cannot be systematic in nature.  
139    In view of the seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter resulting from a measure involving the general and indiscriminate retention of data, it must be ensured that recourse to such a measure is in fact limited to situations in which there is a serious threat to national security as referred to in paragraphs 135 and 136 of the present judgment. For that purpose, it is essential that decisions giving an instruction to providers of electronic communications services to carry out such data retention be subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed.  
–         
Legislative measures providing for the preventive retention of traffic and location data for the purposes of combating crime and safeguarding public security  
140    As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general (see, to that effect, judgments of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 102, and of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraphs 56 and 57; Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 149).  
141    National legislation providing for the general and indiscriminate retention of traffic and location data for the purpose of combating serious crime exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 107).  
142    In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of that data is essential for the right to respect for private life. Thus, having regard, first, to the deterrent effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the Charter, referred to in paragraph 118 above, which is liable to result from the retention of that data, and, second, to the seriousness of the interference entailed by such retention, it is necessary, within a democratic society, that retention be the exception and not the rule, as provided for in the system established by Directive 2002/58, and that the data not be retained systematically and continuously. That conclusion applies even having regard to the objectives of combating serious crime and preventing serious threats to public security and to the importance to be attached to them.  
143    In addition, the Court has emphasised that legislation providing for the general and indiscriminate retention of traffic and location data covers the electronic communications of practically the entire population without any differentiation, limitation or exception being made in the light of the objective pursued. Such legislation, in contrast to the requirement mentioned in paragraph 133 above, is comprehensive in that it affects all persons using electronic communications services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating serious crime and, in particular, without there being any relationship between the data whose retention is provided for and a threat to public security (see, to that effect, judgments of 8 April 2014,   
Digital Rights  
, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 and 58, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 105).  
144    In particular, as the Court has previously held, such legislation is not restricted to retention in relation to (i) data pertaining to a time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to combating serious crime (see, to that effect, judgments of 8 April 2014,   
Digital Rights  
, C-293/12 and C-594/12, EU:C:2014:238, paragraph 59, and of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 106).  
145    Even the positive obligations of the Member States which may arise, depending on the circumstances, from Articles 3, 4 and 7 of the Charter and relating, as pointed out in paragraphs 126 and 128 of the present judgment, to the establishment of rules to facilitate effective action to combat criminal offences cannot have the effect of justifying interference that is as serious as that entailed by legislation providing for the retention of traffic and location data with the fundamental rights, enshrined in Articles 7 and 8 of the Charter, of practically the entire population, without there being a link, at least an indirect one, between the data of the persons concerned and the objective pursued.  
146    By contrast, in accordance with what has been stated in paragraphs 142 to 144 of the present judgment, and having regard to the balance that must be struck between the rights and interests at issue, the objectives of combating serious crime, preventing serious attacks on public security and, a fortiori, safeguarding national security are capable of justifying – given their importance, in the light of the positive obligations mentioned in the preceding paragraph to which the Cour constitutionnelle (Constitutional Court, Belgium), referred, inter alia – the particularly serious interference entailed by the targeted retention of traffic and location data.  
147    Thus, as the Court has previously held, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data for the purposes of combating serious crime, preventing serious threats to public security and equally of safeguarding national security, provided that such retention is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 108).  
148    As regards the limits to which such a data retention measure must be subject, these may, in particular, be determined according to the categories of persons concerned, since Article 15(1) of Directive 2002/58 does not preclude legislation based on objective evidence which makes it possible to target persons whose traffic and location data is likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111).  
149    In that regard, it must be made clear that the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective evidence, as posing a threat to public or national security in the Member State concerned.  
150    The limits on a measure providing for the retention of traffic and location data may also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111). Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas.  
151    In order to ensure that the interference entailed by the targeted retention measures described in paragraphs 147 to 150 of the present judgment complies with the principle of proportionality, their duration must not exceed what is strictly necessary in the light of the objective pursued and the circumstances justifying them, without prejudice to the possibility of extending those measures should such retention continue to be necessary.  
–         
Legislative measures providing for the preventive retention of IP addresses and data relating to civil identity for the purposes of combating crime and safeguarding public security  
152    It should be noted that although IP addresses are part of traffic data, they are generated independently of any particular communication and mainly serve to identify, through providers of electronic communications services, the natural person who owns the terminal equipment from which an Internet communication is made. Thus, in relation to email and Internet telephony, provided that only the IP addresses of the source of the communication are retained and not the IP addresses of the recipient of the communication, those addresses do not, as such, disclose any information about third parties who were in contact with the person who made the communication. That category of data is therefore less sensitive than other traffic data.  
153    However, since IP addresses may be used, among other things, to track an Internet user’s complete clickstream and, therefore, his or her entire online activity, that data enables a detailed profile of the user to be produced. Thus, the retention and analysis of those IP addresses which is required for such tracking constitute a serious interference with the fundamental rights of the Internet user enshrined in Articles 7 and 8 of the Charter, which may have a deterrent effect as mentioned in paragraph 118 of the present judgment.  
154    In order to strike a balance between the rights and interests at issue as required by the case-law cited in paragraph 130 of the present judgment, account must be taken of the fact that, where an offence is committed online, the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified. To that consideration must be added the fact that the retention of IP addresses by providers of electronic communications services beyond the period for which that data is assigned does not, in principle, appear to be necessary for the purpose of billing the services at issue, with the result that the detection of offences committed online may therefore prove impossible without recourse to a legislative measure under Article 15(1) of Directive 2002/58, something which several governments mentioned in their observations to the Court. As those governments argued, that may occur, inter alia, in cases involving particularly serious child pornography offences, such as the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1).  
155    In those circumstances, while it is true that a legislative measure providing for the retention of the IP addresses of all natural persons who own terminal equipment permitting access to the Internet would catch persons who at first sight have no connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with the objectives pursued, and it is also true, in accordance with what has been stated in paragraph 109 of the present judgment, that Internet users are entitled to expect, under Articles 7 and 8 of the Charter, that their identity will not, in principle, be disclosed, a legislative measure providing for the general and indiscriminate retention of only IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of that data.  
156    In the light of the seriousness of the interference entailed by that retention with the fundamental rights enshrined in Articles 7 and 8 of the Charter, only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying that interference. Moreover, the retention period must not exceed what is strictly necessary in the light of the objective pursued. Finally, a measure of that nature must establish strict conditions and safeguards concerning the use of that data, particularly via tracking, with regard to communications made and activities carried out online by the persons concerned.  
157    Concerning, last, data relating to the civil identity of users of electronic communications systems, that data does not, in itself, make it possible to ascertain the date, time, duration and recipients of the communications made, or the locations where those communications took place or their frequency with specific people during a given period, with the result that it does not provide, apart from the contact details of those users, such as their addresses, any information on the communications sent and, consequently, on the users’ private lives. Thus, the interference entailed by the retention of that data cannot, in principle, be classified as serious (see, to that effect, judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraphs 59 and 60).  
158    It follows that, in accordance with what has been stated in paragraph 140 of the present judgment, legislative measures concerning the processing of that data as such, including the retention of and access to that data solely for the purpose of identifying the user concerned, and without it being possible for that data to be associated with information on the communications made, are capable of being justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general, to which the first sentence of Article 15(1) of Directive 2002/58 refers (see, to that effect, judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 62).  
159    In those circumstances, having regard to the balance that must be struck between the rights and interests at issue, and for the reasons set out in paragraphs 131 and 158 of the present judgment, it must be held that, even in the absence of a connection between all users of electronic communications systems and the objectives pursued, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude a legislative measure which requires providers of electronic communications services, without imposing a specific time limit, to retain data relating to the civil identity of all users of electronic communications systems for the purposes of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security, there being no need for the criminal offences or the threats to or acts having adverse effects on public security to be serious.  
–         
Legislative measures providing for the expedited retention of traffic and location data for the purpose of combating serious crime  
160    With regard to traffic and location data processed and stored by providers of electronic communications services on the basis of Articles 5, 6 and 9 of Directive 2002/58 or on the basis of legislative measures taken under Article 15(1) of that directive, as described in paragraphs 134 to 159 of the present judgment, it should be noted that that data must, in principle, be erased or made anonymous, depending on the circumstances, at the end of the statutory periods within which that data must be processed and stored in accordance with the national provisions transposing that directive.  
161    However, during that processing and storage, situations may arise in which it becomes necessary to retain that data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may reasonably be suspected.  
162    In that regard, the Council of Europe’s Convention on Cybercrime of 23 November 2001 (European Treaty Series – No. 185), which was signed by the 27 Member States and ratified by 25 of them and has as its objective to facilitate the fight against criminal offences committed using computer networks, provides, in Article 14, that the parties to the convention are to adopt, for the purpose of specific criminal investigations or proceedings, certain measures concerning traffic data already stored, such as the expedited preservation of that data. In particular, Article 16(1) of that convention stipulates that the parties to that convention are to adopt such legislative measures as may be necessary to enable their competent authorities to order or similarly obtain the expedited preservation of traffic data that has been stored by means of a computer system, in particular where there are grounds to believe that that data is particularly vulnerable to loss or modification.  
163    In a situation such as the one described in paragraph 161 of the present judgment, in the light of the balance that must be struck between the rights and interests at issue referred to in paragraph 130 of the present judgment, it is permissible for Member States to provide, in legislation adopted pursuant to Article 15(1) of Directive 2002/58, for the possibility of instructing, by means of a decision of the competent authority which is subject to effective judicial review, providers of electronic communications services to undertake the expedited retention of traffic and location data at their disposal for a specified period of time.  
164    To the extent that the purpose of such expedited retention no longer corresponds to the purpose for which that data was initially collected and retained and since any processing of data must, under Article 8(2) of the Charter, be consistent with specified purposes, Member States must make clear, in their legislation, for what purpose the expedited retention of data may occur. In the light of the serious nature of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter which such retention may entail, only action to combat serious crime and, a fortiori, the safeguarding of national security are such as to justify such interference. Moreover, in order to ensure that the interference entailed by a measure of that kind is limited to what is strictly necessary, first, the retention obligation must relate only to traffic and location data that may shed light on the serious criminal offences or the acts adversely affecting national security concerned. Second, the duration for which such data is retained must be limited to what is strictly necessary, although that duration can be extended where the circumstances and the objective pursued by that measure justify doing so.  
165    In that regard, such expedited retention need not be limited to the data of persons specifically suspected of having committed a criminal offence or acts adversely affecting national security. While it must comply with the framework established by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, and taking into account the findings in paragraph 133 above, such a measure may, at the choice of the legislature and subject to the limits of what is strictly necessary, be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that that data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, his or her social or professional circle, or even specified geographical areas, such as the place where the offence or act adversely affecting national security at issue was committed or prepared. Additionally, the competent authorities must be given access to the data thus retained in observance of the conditions that emerge from the case-law on how Directive 2002/58 is to be interpreted (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 118 to 121 and the case-law cited).  
166    It should also be added that, as is clear, in particular, from paragraphs 115 and 133 above, access to traffic and location data retained by providers in accordance with a measure taken under Article 15(1) of Directive 2002/58 may, in principle, be justified only by the public interest objective for which those providers were ordered to retain that data. It follows, in particular, that access to such data for the purpose of prosecuting and punishing an ordinary criminal offence may in no event be granted where the retention of such data has been justified by the objective of combating serious crime or, a fortiori, by the objective of safeguarding national security. However, in accordance with the principle of proportionality, as mentioned in paragraph 131 above, access to data retained for the purpose of combating serious crime may, provided that the substantive and procedural conditions associated with such access referred to in the previous paragraph are observed, be justified by the objective of safeguarding national security.  
167    In that regard, it is permissible for Member States to specify in their legislation that access to traffic and location data may, subject to those same substantive and procedural conditions, be permitted for the purpose of combating serious crime or safeguarding national security where that data is retained by a provider in a manner that is consistent with Articles 5, 6 and 9 or Article 15(1) of Directive 2002/58.  
168    In the light of all of the above considerations, the answer to question 1 in Cases C-511/18 and C-512/18 and questions 1 and 2 in Case C-520/18 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data. By contrast, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that:  
–        allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;  
–        provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;  
–        provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period that is limited in time to what is strictly necessary;  
–        provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;  
–        allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,  
provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.  
   
Questions  
   
2 and 3 in Case C  
-  
511/18  
169    By questions 2 and 3 in Case C-511/18, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires providers of electronic communications services to implement, on their networks, measures allowing, first, the automated analysis and real-time collection of traffic and location data and, second, real-time collection of technical data concerning the location of the terminal equipment used, but which makes no provision for the persons concerned by that processing and that collection to be notified thereof.  
170    The referring court notes that the intelligence gathering techniques provided for in Articles L. 851-2 to L. 851-4 of the CSI do not impose on providers of electronic communications services a specific obligation to retain traffic and location data. With regard, in particular, to the automated analysis referred to in Article L. 851-3 of the CSI, the referring court observes that the aim of that processing is to detect, according to criteria established for that purpose, links that might constitute a terrorist threat. As for the real-time collection referred to in Article L. 851-2 of the CSI, that court notes that such collection concerns exclusively one or more persons who have been identified in advance as potentially having a link to a terrorist threat. According to that same court, those two techniques may be implemented only with a view to preventing terrorism and cover the data referred to in Articles L. 851-1 and R. 851-5 of the CSI.  
171    As a preliminary point, it should be noted that the fact that, according to Article L. 851-3 of the CSI, the automated analysis that it provides for does not, as such, allow the users whose data is being analysed to be identified, does not prevent such data from being classified as ‘personal data’. Since the procedure provided for in point IV of that provision allows the person or persons concerned by the data, the automated analysis of which has shown that there may be a terrorist threat, to be identified at a later stage, all persons whose data has been the subject of automated analysis can still be identified from that data. According to the definition of personal data in Article 4(1) of Regulation 2016/679, information relating, inter alia, to an identifiable person constitutes personal data.  
   
Automated analysis of traffic and location data  
172    It is clear from Article L. 851-3 of the CSI that the automated analysis for which it provides corresponds, in essence, to a screening of all the traffic and location data retained by providers of electronic communications services, which is carried out by those providers at the request of the competent national authorities applying the parameters set by the latter. It follows that all data of users of electronic communications systems is verified if it corresponds to those parameters. Therefore, such automated analysis must be considered as involving, for the providers of electronic communications services concerned, the undertaking on behalf of the competent authority of general and indiscriminate processing, in the form of the use of that data with the assistance of an automated operation, within the meaning of Article 4(2) of Regulation 2016/679, covering all traffic and location data of all users of electronic communications systems. That processing is independent of the subsequent collection of data relating to the persons identified following that automated analysis, such collection being authorised on the basis of Article L. 851-3, IV, of the CSI.  
173    National legislation authorising such automated analysis of traffic and location data derogates from the obligation of principle, established in Article 5 of Directive 2002/58, to ensure the confidentiality of electronic communications and related data. Such legislation also constitutes interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, regardless of how that data is used subsequently. Finally, as was stated in the case-law cited in paragraph 118 of the present judgment, such legislation is likely to have a deterrent effect on the exercise of freedom of expression, which is enshrined in Article 11 of the Charter.  
174    Moreover, the interference resulting from the automated analysis of traffic and location data, such as that at issue in the main proceedings, is particularly serious since it covers, generally and indiscriminately, the data of persons using electronic communication systems. That finding is all the more justified given that, as is clear from the national legislation at issue in the main proceedings, the data that is the subject of the automated analysis is likely to reveal the nature of the information consulted online. In addition, such automated analysis is applied generally to all persons who use electronic communication systems and, consequently, applies also to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with terrorist activities.  
175    With regard to the justification for such interference, the requirement, established in Article 52(1) of the Charter, that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits that interference with those rights must itself define the scope of the limitation on the exercise of the right concerned (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited).  
176    In addition, in order to meet the requirement of proportionality recalled in paragraphs 130 and 131 of the present judgment, according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, national legislation governing the access of the competent authorities to retained traffic and location data must comply with the requirements that emerge from the case-law cited in paragraph 132 of the present judgment. In particular, such legislation cannot be limited to requiring that the authorities’ access to such data should correspond to the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (see, by analogy, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 192 and the case-law cited).  
177    In that regard, it should be noted that the particularly serious interference that is constituted by the general and indiscriminate retention of traffic and location data, as referred to in the findings in paragraphs 134 to 139 of the present judgment, and the particularly serious interference constituted by the automated analysis of that data can meet the requirement of proportionality only in situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration of that retention is limited to what is strictly necessary.  
178    In situations such as those referred to in the previous paragraph, the implementation of automated analysis of the traffic and location data of all users of electronic communications systems, for a strictly limited period, may be considered to be justified in the light of the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.  
179    That being said, in order to guarantee that such a measure is actually limited to what is strictly necessary in order to protect national security and, more particularly, to prevent terrorism, in accordance with what was held in paragraph 139 of the present judgment, it is essential that the decision authorising automated analysis be subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed.  
180    In that regard, it should be noted that the pre-established models and criteria on which that type of data processing are based should be, first, specific and reliable, making it possible to achieve results identifying individuals who might be under a reasonable suspicion of participation in terrorist offences and, second, should be non-discriminatory (see, to that effect, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 172).  
181    In addition, it must be noted that any automated analysis carried out on the basis of models and criteria founded on the premiss that racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information about a person’s health or sex life could, in themselves and regardless of the individual conduct of that person, be relevant in order to prevent terrorism would infringe the rights guaranteed in Articles 7 and 8 of the Charter, read in conjunction with Article 21 thereof. Therefore, pre-established models and criteria for the purposes of an automated analysis that has as its objective the prevention of terrorist activities that constitute a serious threat to national security cannot be based on that sensitive data in isolation (see, to that effect, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraph 165).  
182    Furthermore, since the automated analyses of traffic and location data necessarily involve some margin of error, any positive result obtained following automated processing must be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the persons concerned is adopted, such as the subsequent real-time collection of traffic and location data, since such a measure cannot be based solely and decisively on the result of automated processing. Similarly, in order to ensure that, in practice, the pre-established models and criteria, the use that is made of them and the databases used are not discriminatory and are limited to that which is strictly necessary in the light of the objective of preventing terrorist activities that constitute a serious threat to national security, a regular re-examination should be undertaken to ensure that those pre-established models and criteria and the databases used are reliable and up to date (see, to that effect, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraphs 173 and 174).  
   
Real-time collection of traffic and location data  
183    The real-time collection of traffic and location data referred to in Article L. 851-2 of the CSI may be individually authorised in respect of a ‘person previously identified as potentially having links to a [terrorist] threat’. Moreover, according to that description, and ‘where there are substantial grounds for believing that one or more persons belonging to the circle of the person to whom the authorisation relates are capable of providing information in respect of the purpose for which the authorisation was granted, authorisation may also be granted individually for each of those persons’.  
184    The data that is the subject of such a measure allows the national competent authorities to monitor, for the duration of the authorisation, continuously and in real time, the persons with whom those persons are communicating, the means that they use, the duration of their communications and their places of residence and movements. It may also reveal the type of information consulted online. Taken as a whole, as is clear from paragraph 117 of the present judgment, that data makes it possible to draw very precise conclusions concerning the private lives of the persons concerned and provides the means to establish a profile of the individuals concerned, information that is no less sensitive, from the perspective of the right to privacy, than the actual content of communications.  
185    With regard to the real-time collection of data referred to in Article L. 851-4 of the CSI, that provision authorises technical data concerning the location of terminal equipment to be collected and transmitted in real time to a department reporting to the Prime Minister. It appears that such data allows the department responsible, at any moment throughout the duration of that authorisation, to locate, continuously and in real time, the terminal equipment used, such as mobile telephones.  
186    Like national legislation authorising the automated analysis of data, national legislation authorising such real-time collection derogates from the obligation of principle, established in Article 5 of Directive 2002/58, to ensure the confidentiality of electronic communications and related data. It therefore also constitutes interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter and is likely to have a deterrent effect on the exercise of freedom of expression, which is guaranteed in Article 11 of the Charter.  
187    It must be emphasised that the interference constituted by the real-time collection of data that allows terminal equipment to be located appears particularly serious, since that data provides the competent national authorities with a means of accurately and permanently tracking the movements of users of mobile telephones. To the extent that that data must therefore be considered to be particularly sensitive, real-time access by the competent authorities to such data must be distinguished from non-real-time access to that data, the first being more intrusive in that it allows for monitoring of those users that is virtually total (see, by analogy, with regard to Article 8 of the ECHR, ECtHR, 8 February 2018,  
 Ben Faiza   
v.   
France  
 CE:ECHR:2018:0208JUD003144612, § 74). The seriousness of that interference is further aggravated where the real-time collection also extends to the traffic data of the persons concerned.  
188    Although the objective of preventing terrorism pursued by the national legislation at issue in the main proceedings is liable, given its importance, to justify interference in the form of the real-time collection of traffic and location data, such a measure may be implemented, taking into account its particularly intrusive nature, only in respect of persons with respect to whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities. With regard to persons falling outside of that category, they may only be the subject of non-real-time access, which may occur, in accordance with the Court’s case-law, only in particular situations, such as those involving terrorist activities, and where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating terrorism (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119 and the case-law cited).  
189    In addition, a decision authorising the real-time collection of traffic and location data must be based on objective criteria provided for in the national legislation. In particular, that legislation must define, in accordance with the case-law cited in paragraph 176 of the present judgment, the circumstances and conditions under which such collection may be authorised and must provide that, as was pointed out in the previous paragraph, only persons with a link to the objective of preventing terrorism may be subject to such collection. In addition, a decision authorising the real-time collection of traffic and location data must be based on objective and non-discriminatory criteria provided for in national legislation. In order to ensure, in practice, that those conditions are observed, it is essential that the implementation of the measure authorising real-time collection be subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding, with that court or body having to satisfy itself, inter alia, that such real-time collection is authorised only within the limits of what is strictly necessary (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 120). In cases of duly justified urgency, the review must take place within a short time.  
   
Notification of persons whose data has been collected or analysed  
190    The competent national authorities undertaking real-time collection of traffic and location data must notify the persons concerned, in accordance with the applicable national procedures, to the extent that and as soon as that notification is no longer liable to jeopardise the tasks for which those authorities are responsible. That notification is, indeed, necessary to enable the persons affected to exercise their rights under Articles 7 and 8 of the Charter to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased, as well as to avail themselves, in accordance with the first paragraph of Article 47 of the Charter, of an effective remedy before a tribunal, that right indeed being explicitly guaranteed in Article 15(2) of Directive 2002/58, read in conjunction with Article 79(1) of Regulation 2016/679 (see, to that effect, judgment of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 121 and the case-law cited, and Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraphs 219 and 220).  
191    With regard to the notification required in the context of automated analysis of traffic and location data, the competent national authority is obliged to publish information of a general nature relating to that analysis without having to notify the persons concerned individually. However, if the data matches the parameters specified in the measure authorising automated analysis and that authority identifies the person concerned in order to analyse in greater depth the data concerning him or her, it is necessary to notify that person individually. That notification must, however, occur only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible (see, by analogy, Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraphs 222 and 224).  
192    In the light of all the foregoing, the answer to questions 2 and 3 in Case C-511/18 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as not precluding national rules which requires providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection, inter alia, of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used, where:  
–        recourse to automated analysis is limited to situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of an effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed; and where  
–        recourse to the real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.  
   
Question  
   
2 in Case C  
-  
512/18  
193    By question 2 in Case C-512/18, the referring court seeks, in essence, to ascertain whether the provisions of Directive 2000/31, read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, inter alia, personal data relating to those services.  
194    While the referring court maintains that such services fall within the scope of Directive 2000/31 rather than within that of Directive 2002/58, it takes the view that Article 15(1) and (2) of Directive 2000/31, read in conjunction with Articles 12 and 14 of the same, does not, in itself, establish a prohibition in principle on data relating to content creation being retained, which can be derogated from only exceptionally. However, that court is uncertain whether that finding can be made given that the fundamental rights enshrined in Articles 6, 7, 8 and 11 of the Charter must necessarily be observed.  
195    In addition, the referring court points out that its question is raised in reference to the obligation to retain provided for in Article 6 of the LCEN, read in conjunction with Decree No 2011-219. The data that must be retained by the service providers concerned on that basis includes, inter alia, data relating to the civil identity of persons who have used those services, such as their surname, forename, their associated postal addresses, their associated email or account addresses, their passwords and, where the subscription to the contract or account must be paid for, the type of payment used, the payment reference, the amount and the date and time of the transaction.  
196    Furthermore, the data that is the subject of the obligation to retain covers the identifiers of subscribers, of connections and of terminal equipment used, the identifiers attributed to the content, the dates and times of the start and end of the connections and operations as well as the types of protocols used to connect to the service and transfer the content. Access to that data, which must be retained for one year, may be requested in the context of criminal and civil proceedings, in order to ensure compliance with the rules governing civil and criminal liability, and in the context of the intelligence collection measures to which Article L. 851-1 of the CSI applies.  
197    In that regard, it should be noted that, in accordance with Article 1(2) of Directive 2000/31, that directive approximates certain national provisions on information society services that are referred to in Article 2(a) of that directive.  
198    It is true that such services include those which are provided at a distance, by means of electronic equipment for the processing and storage of data, at the individual request of a recipient of services, and normally in return for remuneration, such as services providing access to the Internet or to a communication network and hosting services (see, to that effect, judgments of 24 November 2011,   
Scarlet Extended  
, C-70/10, EU:C:2011:771, paragraph 40; of 16 February 2012,   
SABAM  
, C-360/10, EU:C:2012:85, paragraph 34; of 15 September 2016,   
Mc Fadden  
, C-484/14, EU:C:2016:689, paragraph 55; and of 7 August 2018,   
SNB-REACT  
, C-521/17, EU:C:2018:639, paragraph 42 and the case-law cited).  
199    However, Article 1(5) of Directive 2000/31 provides that that directive is not to apply to questions relating to information society services covered by Directives 95/46 and 97/66. In that regard, it is clear from recitals 14 and 15 of Directive 2000/31 that the protection of the confidentiality of communications and of natural persons with regard to the processing of personal data in the context of information society services are governed only by Directives 95/46 and 97/66, the latter of which prohibits, in Article 5 thereof, all forms of interception or surveillance of communications, in order to protect confidentiality.  
200    Questions related to the protection of the confidentiality of communications and personal data must be assessed on the basis of Directive 2002/58 and Regulation 2016/679, which replaced Directive 97/66 and Directive 95/46 respectively, and it should be noted that the protection that Directive 2000/31 is intended to ensure cannot, in any event, undermine the requirements under Directive 2002/58 and Regulation 2016/679 (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 57).  
201    The obligation imposed by the national legislation referred to in paragraph 195 of the present judgment on providers of access to online public communication services and hosting service providers requiring them to retain personal data relating to those services must, therefore – as the Advocate General proposed in point 141 of his Opinion in Joined Cases   
La Quadrature du Net and Others  
 (C-511/18 and C-512/18, EU:C:2020:6) – be assessed on the basis of Directive 2002/58 or Regulation 2016/679.  
202    Accordingly, depending on whether the provision of services covered by that national legislation falls within the scope of Directive 2002/58 or not, it is to be governed either by that directive, specifically by Article 15(1) thereof, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, or by Regulation 2016/679, specifically by Article 23(1) of that regulation, read in the light of the same articles of the Charter.  
203    In the present instance, it is conceivable, as the European Commission submitted in its written observations, that some of the services to which the national legislation referred to in paragraph 195 of the present judgment is applicable constitute electronic communications services within the meaning of Directive 2002/58, which is for the referring court to verify.  
204    In that regard, Directive 2002/58 covers electronic communications services that satisfy the conditions set out in Article 2(c) of Directive 2002/21, to which Article 2 of Directive 2002/58 refers and which defines an electronic communications service as ‘a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting’. As regards information society services, such as those referred to in paragraphs 197 and 198 of the present judgment and covered by Directive 2000/31, they are electronic communications services to the extent that they consist wholly or mainly in the conveyance of signals on electronic communications networks (see, to that effect, judgment of 5 June 2019,   
Skype Communications  
, C-142/18, EU:C:2019:460, paragraphs 47 and 48).  
205    Therefore, Internet access services, which appear to be covered by the national legislation referred to in paragraph 195 of the present judgment, constitute electronic communications services within the meaning of Directive 2002/21, as is confirmed by recital 10 of that directive (see, to that effect, judgment of 5 June 2019,   
Skype Communications  
, C-142/18, EU:C:2019:460, paragraph 37). That is also the case for web-based email services, which, it appears, could conceivably also fall under that national legislation, since, on a technical level, they also involve wholly or mainly the conveyance of signals on electronic communications networks (see, to that effect, judgment of 13 June 2019,   
Google  
, C-193/18, EU:C:2019:498, paragraphs 35 and 38).  
206    With regard to the requirements resulting from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, it is appropriate to refer back to all of the findings and assessments made in the context of the answer given to question 1 in each of Cases C-511/18 and C-512/18 and to questions 1 and 2 in Case C-520/18.  
207    As regards the requirements stemming from Regulation 2016/679, it should be noted that the purpose of that regulation is, inter alia, as is apparent from recital 10 thereof, to ensure a high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 101).  
208    To that end, any processing of personal data must, subject to the derogations permitted in Article 23 of Regulation 2016/679, observe the principles governing the processing of personal data and the rights of the person concerned set out, respectively, in Chapters II and III of that regulation. In particular, any processing of personal data must, first, comply with the principles set out in Article 5 of that regulation and, second, satisfy the lawfulness conditions listed in Article 6 of that regulation (see, by analogy, with regard to Directive 95/46, judgment of 30 May 2013,   
Worten  
, C-342/12, EU:C:2013:355, paragraph 33 and the case-law cited).  
209    With regard, more specifically, to Article 23(1) of Regulation 2016/679, that provision, much like Article 15(1) of Directive 2002/58, allows Member States to restrict, for the purposes of the objectives that it provides for and by means of legislative measures, the scope of the obligations and rights that are referred to therein ‘when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard’ the objective pursued. Any legislative measure adopted on that basis must, in particular, comply with the specific requirements set out in Article 23(2) of that regulation.  
210    Accordingly, Article 23(1) and (2) of Regulation 2016/679 cannot be interpreted as being capable of conferring on Member States the power to undermine respect for private life, disregarding Article 7 of the Charter, or any of the other guarantees enshrined therein (see, by analogy, with regard to Directive 95/46, judgment of 20 May 2003,   
Österreichischer Rundfunk and Others  
, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 91). In particular, as is the case for Article 15(1) of Directive 2002/58, the power conferred on Member States by Article 23(1) of Regulation 2016/679 may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (see, by analogy, with regard to Directive 95/46, judgment of 7 November 2013,   
IPI  
, C-473/12, EU:C:2013:715, paragraph 39 and the case-law cited).  
211    It follows that the findings and assessments made in the context of the answer given to question 1 in each of Cases C-511/18 and C-512/18 and to questions 1 and 2 in Case C-520/18 apply,   
mutatis mutandis  
, to Article 23 of Regulation 2016/679.  
212    In the light of the foregoing, the answer to question 2 in Case C-512/18 is that Directive 2000/31 must be interpreted as not being applicable in the field of the protection of the confidentiality of communications and of natural persons as regards the processing of personal data in the context of information society services, such protection being governed by Directive 2002/58 or by Regulation 2016/679, as appropriate. Article 23(1) of Regulation 2016/679, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services.  
   
Question  
   
3 in Case C  
-  
520/18  
213    By question 3 in Case C-520/18, the referring court seeks, in essence, to ascertain whether a national court may apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make under that law in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, pursuing the objectives of safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data, owing to the fact that that legislation is incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.  
214    The principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State bodies to give full effect to the various EU provisions, and the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States (judgments of 15 July 1964,   
Costa  
, 6/64, EU:C:1964:66, pp. 593 and 594, and of 19 November 2019,   
A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)  
, C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraphs 157 and 158 and the case-law cited).  
215    In the light of the primacy principle, where it is unable to interpret national law in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means (judgments of 22 June 2010,   
Melki and Abdeli  
, C-188/10 and C-189/10, EU:C:2010:363, paragraph 43 and the case-law cited; of 24 June 2019,   
Popławski  
, C-573/17, EU:C:2019:530, paragraph 58; and of 19 November 2019,   
A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)  
, C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraph 160).  
216    Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested (see, to that effect, judgments of 23 October 2012,   
Nelson and Others  
, C-581/10 and C-629/10, EU:C:2012:657, paragraphs 89 and 91; of 23 April 2020,   
Herst  
, C-401/18, EU:C:2020:295, paragraphs 56 and 57; and of 25 June 2020,   
A and Others (Wind turbines at Aalter and Nevele)  
, C-24/19, EU:C:2020:503, paragraph 84 and the case-law cited).  
217    The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (see, to that effect, judgment of 29 July 2019,   
Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen  
, C-411/17, EU:C:2019:622, paragraph 177 and the case-law cited).  
218    However, the Court has held, in a case concerning the lawfulness of measures adopted in breach of the obligation under EU law to conduct a prior assessment of the impact of a project on the environment and on a protected site, that if domestic law allows it, a national court may, by way of exception, maintain the effects of such measures where such maintenance is justified by overriding considerations relating to the need to nullify a genuine and serious threat of interruption in the electricity supply in the Member State concerned, which cannot be remedied by any other means or alternatives, particularly in the context of the internal market, and continues only for as long as is strictly necessary to remedy the breach (see, to that effect, judgment of 29 July 2019,   
Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen  
, C-411/17, EU:C:2019:622, paragraphs 175, 176, 179 and 181).  
219    However, unlike a breach of a procedural obligation such as the prior assessment of the impact of a project in the specific field of environmental protection, a failure to comply with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure referred to in the preceding paragraph. Maintaining the effects of national legislation such as that at issue in the main proceedings would mean that the legislation would continue to impose on providers of electronic communications services obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data has been retained.  
220    Therefore, the referring court cannot apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make under that law in respect of the national legislation at issue in the main proceedings.  
221    That said, in their observations submitted to the Court, VZ, WY and XX contend that question 3 implicitly yet necessarily asks whether EU law precludes the use, in criminal proceedings, of information and evidence obtained as a result of the general and indiscriminate retention of traffic and location data in breach of that law.  
222    In that regard, and in order to give a useful answer to the referring court, it should be recalled that, as EU law currently stands, it is, in principle, for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of information and evidence obtained by such retention of data contrary to EU law.  
223    The Court has consistently held that, in the absence of EU rules on the matter, it is for the national legal order of each Member State to establish, in accordance with the principle of procedural autonomy, procedural rules for actions intended to safeguard the rights that individuals derive from EU law, provided, however, that those rules are no less favourable than the rules governing similar domestic actions (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness) (see, to that effect, judgments of 6 October 2015,   
Târşia  
, C-69/14, EU:C:2015:662, paragraphs 26 and 27; of 24 October 2018,   
XC and Others  
, C-234/17, EU:C:2018:853, paragraphs 21 and 22 and the case-law cited; and of 19 December 2019,   
Deutsche Umwelthilfe  
, C-752/18, EU:C:2019:1114, paragraph 33).  
224    As regards the principle of equivalence, it is for the national court hearing criminal proceedings based on information or evidence obtained in contravention of the requirements stemming from Directive 2002/58 to determine whether national law governing those proceedings lays down less favourable rules on the admissibility and use of such information and evidence than those governing information and evidence obtained in breach of domestic law.  
225    As for the principle of effectiveness, it should be noted that the objective of national rules on the admissibility and use of information and evidence is, in accordance with the choices made by national law, to prevent information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences. That objective may be achieved under national law not only by prohibiting the use of such information and evidence, but also by means of national rules and practices governing the assessment and weighting of such material, or by factoring in whether that material is unlawful when determining the sentence.  
226    That said, it is apparent from the Court’s case-law that in deciding whether to exclude information and evidence obtained in contravention of the requirements of EU law, regard must be had, in particular, to the risk of breach of the adversarial principle and, therefore, the right to a fair trial entailed by the admissibility of such information and evidence (see, to that effect, judgment of 10 April 2003,   
Steffensen  
, C-276/01, EU:C:2003:228, paragraphs 76 and 77). If a court takes the view that a party is not in a position to comment effectively on evidence pertaining to a field of which the judges have no knowledge and is likely to have a preponderant influence on the findings of fact, it must find an infringement of the right to a fair trial and exclude that evidence to avoid such an infringement (see, to that effect, judgment of 10 April 2003,   
Steffensen  
, C-276/01, EU:C:2003:228, paragraphs 78 and 79).  
227    Therefore, the principle of effectiveness requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.  
228    In the light of the foregoing, the answer to question 3 in Case C-520/18 is that a national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality, which it is bound to make under that law, in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter. Article 15(1), interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.  
   
Costs  
229    Since these proceedings are, for the parties to the main proceedings, a step in the actions pending before the national courts, the decision on costs is a matter for those courts. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding legislative measures which, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data. By contrast, Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, does not preclude legislative measures that:  
–          
allow, for the purposes of safeguarding national security, recourse to   
an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;  
–          
provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;  
–          
provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period that is limited in time to what is strictly necessary;  
–          
provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;  
–          
allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,  
provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.  
2.        
Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as not precluding national rules which requires providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection, inter alia, of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used, where:  
–          
recourse to automated analysis is limited to situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of an effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed; and where  
–          
recourse to the real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.  
3.        
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’), must be interpreted as not being applicable in the field of the protection of the confidentiality of communications and of natural persons as regards the processing of personal data in the context of information society services, such protection being governed by Directive 2002/58, as amended by Directive 2009/136, or by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as appropriate. Article 23(1) of Regulation 2016/679, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services.  
4.        
A national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality, which it is bound to make under that law, in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights. Article 15(1), interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.

ID: ab7329a4-c7c3-4c71-bc26-4498345e2e67

of 4 May 2023, C-487/21 (  
Österreichische Datenschutzbehörde and CRIF  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
   
JUDGMENT OF THE COURT (First Chamber)  
4 May 2023 (\*)  
(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Data subject’s right of access to his or her data undergoing processing – Article 15(3) – Provision of a copy of the data – Concept of ‘copy’ – Concept of ‘information’)  
In Case C-487/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Austria), made by decision of 9 August 2021, received at the Court on 9 August 2021, in the proceedings  
F.F.  
v  
Österreichische Datenschutzbehörde,  
intervening party:  
CRIF GmbH,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, P.G. Xuereb, T. von Danwitz, A. Kumin and I. Ziemele (Rapporteur), Judges,  
Advocate General: G. Pitruzzella,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        F.F., by M. Schrems,  
–        Österreichische Datenschutzbehörde, by A. Jelinek and M. Schmidl, acting as Agents,  
–        CRIF GmbH, by L. Feiler and M. Raschhofer, Rechtsanwälte,  
–        the Austrian Government, by G. Kunnert, A. Posch and J. Schmoll, acting as Agents,  
–        the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by M. Russo, avvocato dello Stato,  
–        the European Commission, by A. Bouchagiar, M. Heller and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 15 December 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
2        The request has been made in proceedings between F.F. and the Österreichische Datenschutzbehörde (Austrian Data Protection Authority; ‘DSB’) concerning DSB’s refusal to require CRIF GmbH to send F.F. a copy of the documents and extracts from databases containing, inter alia, his personal data undergoing processing.  
   
Legal context  
3        Recitals 10, 11, 26, 58, 60 and 63 of the GDPR are worded as follows:  
‘(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the [European] Union. …  
(11)      Effective protection of personal data throughout the [European] Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data …  
…  
(26)      The principles of data protection should apply to any information concerning an identified or identifiable natural person. … To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. …  
…  
(58)      The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language … be used.  
…  
(60)      The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. …  
…  
(63)      A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. … Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. …’  
4        Article 4 of that regulation states:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person …; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means …;  
…’  
5        Article 12 of the GDPR, entitled ‘Transparent information, communication and modalities for the exercise of the rights of the data subject’, provides:  
‘1.      The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.  
…  
3.      The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. … Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.  
…’  
6        Pursuant to Article 15 of the GDPR, headed ‘Right of access by the data subject’:  
‘1.      The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:  
(a)      the purposes of the processing;  
(b)      the categories of personal data concerned;  
(c)      the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;  
(d)      where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;  
(e)      the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;  
(f)      the right to lodge a complaint with a supervisory authority;  
(g)      where the personal data are not collected from the data subject, any available information as to their source;  
(h)      the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.  
2.      Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.  
3.      The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.  
4.      The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.’  
7        Article 16 of the GDPR, headed ‘Right to rectification’, provides:  
‘The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.’  
8        Article 17 of that regulation, entitled ‘Right to erasure (“right to be forgotten”)’, states in paragraph 1 thereof:  
‘The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay …  
…’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
9        CRIF is a business consulting agency that provides, at the request of its clients, information on the creditworthiness of third parties. It was for that purpose that it processed the personal data of the applicant in the main proceedings.  
10      On 20 December 2018, the applicant applied to CRIF, on the basis of Article 15 of the GDPR, for access to the personal data concerning him. In addition, he asked to be provided with a copy of the documents, namely emails and database extracts containing, inter alia, his data, ‘in a standard technical format’.  
11      In response to that request, CRIF sent the applicant in the main proceedings, in summary form, the list of his personal data undergoing processing.  
12      Being of the view that CRIF should have sent him a copy of all the documents containing his data, such as emails and database extracts, the applicant in the main proceedings lodged a complaint with DSB.  
13      By decision of 11 September 2019, DSB rejected that complaint, taking the view that CRIF had not in any way infringed the right of access of the applicant in the main proceedings to his personal data.  
14      The referring court, hearing the action brought by the applicant in the main proceedings against that decision, is uncertain as to the scope of the first sentence of Article 15(3) of the GDPR. It wonders in particular whether the obligation laid down in that provision to provide a ‘copy’ of the personal data is fulfilled where the controller transmits the personal data in the form of a summary table or whether that obligation also entails the transmission of document extracts or entire documents, as well as database extracts, in which those data are reproduced.  
15      More specifically, the referring court asks whether the first sentence of Article 15(3) of the GDPR merely defines the form in which the right of access to information referred to in Article 15(1) of that regulation must be guaranteed, or whether that first provision enshrines an autonomous right of the data subject to access information relating to the context in which that person’s data are processed, in the form of copies of document extracts, or entire documents or database extracts which contain, inter alia, those data.  
16      In addition, the referring court asks whether the term ‘information’, which appears in the third sentence of Article 15(3) of the GDPR, includes the information referred to in Article 15(1)(a) to (h) of that regulation, or even additional information such as metadata related to the data, or whether it covers only the ‘personal data undergoing processing’ referred to in the first sentence of Article 15(3) of that regulation.  
17      In those circumstances, the Bundesverwaltungsgericht (Federal Administrative Court, Austria) decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Is the term “copy” in Article 15(3) of [the GDPR] to be interpreted as meaning a photocopy, a facsimile or an electronic copy of [an] (electronic) item of data, or does it also cover an “  
Abschrift  
”, a “double” (“  
duplicata  
”) or a “transcript”, in line with the understanding of the term in German, French and English dictionaries?  
(2)      Is the first sentence of Article 15(3) of the GDPR, according to which “the controller shall provide a copy of the personal data undergoing processing”, to be interpreted as affording a general right for a data subject to obtain a copy of – also – entire documents in which the personal data of that data subject are processed, or to receive a copy of a database extract if the personal data are processed in such a database, or does the data subject have a right – only – to an exact reproduction of the personal data about which information is to be provided pursuant to Article 15(1) of the GDPR?  
(3)      In the event that Question 2 is answered to the effect that the data subject has a right only to an exact reproduction of the personal data about which information is to be provided pursuant to Article 15(1) of the GDPR, is the first sentence of Article 15(3) of the GDPR to be interpreted as meaning that, depending on the nature of the data processed (for example in relation to the diagnoses, examination results and assessments mentioned in recital 63 or documents in relation to an examination within the meaning of the judgment of the Court of Justice of 20 December 2017,   
Nowak  
,  
   
C-434/16, EU:C:2017:994) and the transparency requirement in Article 12(1) of the GDPR, it may nevertheless be necessary in individual cases to make text passages or entire documents available to the data subject?  
(4)      Is the term “information” which, pursuant to the third sentence of Article 15(3) of the GDPR, “where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, … shall be provided in a commonly used electronic form”, to be interpreted as referring solely to the “personal data undergoing processing” mentioned in the first sentence of Article 15(3) of the GDPR?  
(a)      If Question 4 is answered in the negative: Is the term “information” which, pursuant to the third sentence of Article 15(3) of the GDPR, “where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, … shall be provided in a commonly used electronic form” to be interpreted as also referring to the information pursuant to Article 15(1)(a) to (h) of the GDPR?  
(b)      If Question 4a also is answered in the negative: Is the term “information” which, pursuant to the third sentence of Article 15(3) of the GDPR, “where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, … shall be provided in a commonly used electronic form” to be interpreted as referring, beyond the “personal data undergoing processing” and the information pursuant to Article 15(1)(a) to (h) of the GDPR, to associated metadata, for example?’  
   
Consideration of the questions referred  
   
The first, second and third questions referred  
18      By its first three questions, which it is appropriate to examine together, the referring court asks, in essence, whether the first sentence of Article 15(3) of the GDPR, read in the light of the transparency requirement laid down in Article 12(1) of that regulation, must be interpreted as meaning that the right to obtain a copy of the personal data undergoing processing means that the data subject must be given not only a copy of those data, but also a copy of extracts from documents or even entire documents or extracts from databases which contain, inter alia, those data. That court is uncertain, in particular, of the extent of that right.  
19      As a preliminary point, it should be recalled that, according to the Court’s settled case-law, in interpreting a provision of EU law, it is necessary to consider not only its wording, by reference to its usual meaning in everyday language, but also the context in which it occurs and the objectives pursued by the rules of which it is part (see, to that effect, judgments of 2 December 2021,   
Vodafone Kabel Deutschland  
, C-484/20, EU:C:2021:975, paragraph 19 and the case-law cited, and of 7 September 2022,   
Staatssecretaris van Justitie en Veiligheid (Nature of the right of residence under Article 20 TFEU)  
, C-624/20, EU:C:2022:639, paragraph 28).  
20      As regards the wording of the first sentence of Article 15(3) of the GDPR, that provision states that the controller ‘shall provide a copy of the personal data undergoing processing’.  
21      Although the GDPR does not contain a definition of the term ‘copy’ thus used, account must be taken of the usual meaning of that term, which refers, as the Advocate General observed in point 30 of his Opinion, to the faithful reproduction or transcription of an original, with the result that a purely general description of the data undergoing processing or a reference to categories of personal data does not correspond to that definition. Furthermore, it is apparent from the wording of the first sentence of Article 15(3) of that regulation that the disclosure obligation relates to the personal data undergoing the processing in question.  
22      Article 4(1) of the GDPR defines the concept of ‘personal data’ as ‘any information relating to an identified or identifiable natural person’ and specifies that ‘an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.  
23      The use of the expression ‘any information’ in the definition of the concept of ‘personal data’ in that provision reflects the aim of the EU legislature to assign a wide scope to that concept, which potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it ‘relates’ to the data subject (see, by analogy, judgment of 20 December 2017,   
Nowak  
, C-434/16, EU:C:2017:994, paragraph 34).  
24      In that regard, it has been held that information relates to an identified or identifiable natural person where, by reason of its content, purpose or effect, it is linked to an identifiable person (see, to that effect, judgment of 20 December 2017,   
Nowak  
, C-434/16, EU:C:2017:994, paragraph 35).  
25      As regards the ‘identifiable’ nature of a natural person, recital 26 of the GDPR states that account should be taken of ‘all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly’.  
26      Thus, as the Advocate General observed, in essence, in points 36 to 39 of his Opinion, the broad definition of the concept of ‘personal data’ covers not only data collected and stored by the controller, but also includes all information resulting from the processing of personal data relating to an identified or identifiable person, such as the assessment of that person’s creditworthiness or his or her ability to pay.  
27      In that respect, it should also be added that the EU legislature intended to give the concept of ‘processing’, as defined in Article 4(2) of the GDPR, a broad scope by using a non-exhaustive list of operations (see, to that effect, judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 35).  
28      Accordingly, it follows from the literal analysis of the first sentence of Article 15(3) of the GDPR that that provision confers on the data subject the right to obtain a faithful reproduction of his or her personal data, understood in a broad sense, that are subject to operations that can be classified as processing carried out by the controller.  
29      That said, it must be held that the wording of that provision does not, in itself, enable an answer to be given to the first three questions in so far as it contains no indication regarding any right to obtain not only a copy of the personal data undergoing processing, but also a copy of extracts from documents or even entire documents or extracts from databases which contain, inter alia, those data.  
30      As regards the context of which the first sentence of Article 15(3) of the GDPR forms part, it should be noted that Article 15 of the GDPR, which is entitled ‘Right of access by the data subject’, defines, in paragraph 1 thereof, the subject matter and scope of the data subject’s right of access and enshrines that data subject’s right to obtain from the controller access to his or her personal data and the information referred to in points (a) to (h) of that paragraph.  
31      Article 15(3) of the GDPR sets out the practical arrangements for the fulfilment of the controller’s obligation, specifying, inter alia, in its first sentence, the form in which that controller must provide the ‘personal data undergoing processing’, namely in the form of a ‘copy’. In addition, the third sentence of that paragraph states that the information is to be provided in a commonly used electronic form where the request is made by electronic means, unless otherwise requested by the data subject.  
32      As a result, Article 15(3) of the GDPR cannot be interpreted as establishing a separate right from that provided for in Article 15(1). Moreover, as the European Commission noted in its written observations, the term ‘copy’ does not relate to a document as such, but to the personal data which it contains and which must be complete. The copy must therefore contain all the personal data undergoing processing.  
33      As regards the objectives pursued by Article 15 of the GDPR, it should be noted that the purpose of the GDPR, as stated in recital 11 thereof, is to strengthen and set out in detail the rights of data subjects. Article 15 of that regulation provides, in that regard, for a right to obtain a copy, unlike the second indent of Article 12(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), which merely required ‘communication … in an intelligible form of the data undergoing processing’. Recital 63 of the GDPR states that ‘a data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing’.  
34      Thus, the right of access provided for in Article 15 of the GDPR must enable the data subject to ensure that the personal data relating to him or her are correct and that they are processed in a lawful manner (see, to that effect, judgment of 12 January 2023,   
Österreichische Post (Information regarding the recipients of personal data)  
, C-154/21, EU:C:2023:3, paragraph 37 and the case-law cited).  
35      In particular, that right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her right to rectification, right to erasure (‘right to be forgotten’) or right to restriction of processing, conferred, respectively, by Articles 16, 17 and 18 of the GDPR, as well as the data subject’s right to object to his or her personal data being processed, laid down in Article 21 of the GDPR, and right of action where he or she suffers damage, laid down in Articles 79 and 82 of the GDPR (judgment of 12 January 2023,   
Österreichische Post (Information regarding the recipients of personal data)  
, C-154/21, EU:C:2023:3, paragraph 38 and the case-law cited).  
36      It should also be noted that recital 60 of the GDPR states that the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes, it being stressed that the controller should provide any other information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed.  
37      Furthermore, in accordance with the principle of transparency, alluded to by the referring court, to which recital 58 of the GDPR refers and which is expressly enshrined in Article 12(1) of that regulation, any information sent to the data subject must be concise, easily accessible and easy to understand, and formulated in clear and plain language.  
38      As the Advocate General stated in points 54 and 55 of his Opinion, it follows from that provision that the controller is obliged to take appropriate measures to provide the data subject with all the information referred to, inter alia, in Article 15 of the GDPR, in a concise, transparent, intelligible and easily accessible form, using plain and clear language, and that the information must be provided in writing or by other means, including, where appropriate, by electronic means, unless the data subject requests that it be provided orally. The purpose of that provision, which is an expression of the principle of transparency, is to ensure that the data subject is able fully to understand the information sent to him or her.  
39      It follows that the copy of the personal data undergoing processing, which the controller must provide pursuant to the first sentence of Article 15(3) of the GDPR, must have all the characteristics necessary for the data subject effectively to exercise his or her rights under that regulation and must, consequently, reproduce those data fully and faithfully.  
40      That interpretation corresponds to the objective of the GDPR, which seeks, inter alia, as is apparent from recital 10 thereof, to ensure a high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union (see, to that effect, judgment of 9 February 2023,   
X-FAB Dresden  
, C-453/21, EU:C:2023:79, paragraph 25 and the case-law cited).  
41      In order to ensure that the information thus provided is easy to understand, as required by Article 12(1) of the GDPR, read in conjunction with recital 58 of that regulation, the reproduction of extracts from documents or even entire documents or extracts from databases which contain, inter alia, the personal data undergoing processing may prove to be essential, as the Advocate General observed in points 57 and 58 of his Opinion, where the contextualisation of the data processed is necessary in order to ensure the data are intelligible.  
42      In particular, where personal data are generated from other data or where such data result from empty fields, that is to say, where there is an absence of information which provides information about the data subject, the context in which the data are processed is an essential element in enabling the data subject to have transparent access and an intelligible presentation of those data.  
43      In any event, in accordance with Article 15(4) of the GDPR, read in conjunction with recital 63 of that regulation, the right to obtain a copy referred to in paragraph 3 of that article must not adversely affect the rights and freedoms of others, including trade secrets or intellectual property, and in particular the copyright protecting the software.  
44      Therefore, as the Advocate General stated in point 61 of his Opinion, in the event of conflict between, on the one hand, exercising the right of full and complete access to personal data and, on the other hand, the rights and freedoms of others, a balance will have to be struck between the rights in question. Wherever possible, means of communicating personal data that do not infringe the rights or freedoms of others should be chosen, bearing in mind that, as follows from recital 63 of the GDPR, ‘the result of those considerations should not be a refusal to provide all information to the data subject’.  
45      In the light of the foregoing considerations, the answer to the first, second and third questions referred is that the first sentence of Article 15(3) of the GDPR  
must be interpreted as meaning that the right to obtain from the controller a copy of the personal data undergoing processing means that the data subject must be given a faithful and intelligible reproduction of all those data. That right entails the right to obtain copies of extracts from documents or even entire documents or extracts from databases which contain, inter alia, those data, if the provision of such a copy is essential in order to enable the data subject to exercise effectively the rights conferred on him or her by that regulation, bearing in mind that account must be taken, in that regard, of the rights and freedoms of others.  
   
The fourth question referred  
46      By the fourth question, the referring court asks, in essence, whether the third sentence of Article 15(3) of the GDPR must be interpreted as meaning that the concept of ‘information’ to which it refers relates exclusively to the personal data of which the controller must provide a copy pursuant to the first sentence of that paragraph, or whether it also refers to all the information referred to in paragraph 1 of that article, or even covers elements going beyond that information, such as metadata.  
47      As was pointed out in paragraph 19 above, in interpreting a provision of EU law, it is necessary to consider not only its wording but also the context in which it occurs and the objectives pursued by the rules of which it forms part.  
48      In that regard, although the third sentence of Article 15(3) of the GDPR merely states that, ‘where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form’, without specifying what is to be understood by the term ‘information’, the first sentence of that paragraph states that ‘the controller shall provide a copy of the personal data undergoing processing’.  
49      Accordingly, it follows from the context of the third sentence of Article 15(3) of the GDPR that the ‘information’ to which it refers necessarily corresponds to the personal data of which the controller must provide a copy in accordance with the first sentence of that paragraph.  
50      Such an interpretation is confirmed by the objectives pursued by Article 15(3) of the GDPR, which are, as recalled in paragraph 31 above, to define the practical arrangements for the fulfilment of the controller’s obligation to provide a copy of the personal data undergoing processing. Consequently, that provision does not create a right separate from that which the data subject enjoys to obtain a faithful and intelligible reproduction of those data, enabling him or her effectively to exercise the rights conferred on him or her by that regulation.  
51      It should be noted that no provision of that regulation establishes a difference in treatment of an application according to the form in which it is submitted, with the result that the scope of the right to obtain a copy cannot vary according to that form.  
52      Furthermore, it should also be noted that, in accordance with Article 12(3) of the GDPR, where the request has been made by electronic means, the information referred to in Article 15, including that referred to in Article 15(1)(a) to (h), is to be provided by electronic means, unless otherwise indicated by the data subject.  
53      In the light of the foregoing considerations, the answer to the fourth question referred is that the third sentence of Article 15(3) of the GDPR  
must be interpreted as meaning that the concept of ‘information’ to which it refers relates exclusively to the personal data of which the controller must provide a copy pursuant to the first sentence of that paragraph.  
   
Costs  
54      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
1.        
The first sentence of Article 15(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),  
must be interpreted as meaning that the right to obtain from the controller a copy of the personal data undergoing processing means that the data subject must be given a faithful and intelligible reproduction of all those data. That right entails the right to obtain copies of extracts from documents or even entire documents or extracts from databases which contain, inter alia, those data, if the provision of such a copy is essential in order to enable the data subject to exercise effectively the rights conferred on him or her by that regulation, bearing in mind that account must be taken, in that regard, of the rights and freedoms of others.  
2.        
The third sentence of Article 15(3) of Regulation 2016/679  
must be interpreted as meaning that the concept of ‘information’ to which it refers relates exclusively to the personal data of which the controller must provide a copy pursuant to the first sentence of that paragraph.

ID: af6074ae-dc6b-4545-83f8-b5c94fc4beae

Judgment of 7 Nov 2013, C-473/12 (  
IPI  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Information to be provided in case of direct collection   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
 Information to be provided in case of indirect collection   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
   
JUDGMENT OF THE COURT (Third Chamber)  
7 November 2013 (\*)  
(Processing of personal data – Directive 95/46/EC – Articles 10 and 11 – Obligation to inform – Article 13(1)(d) and (g) – Exceptions – Scope of exceptions – Private detectives acting for the supervisory body of a regulated profession – Directive 2002/58/EC – Article 15(1))  
In Case C-473/12,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Cour constitutionnelle (Belgium), made by decision of 10 October 2012, received at the Court on 22 October 2012, in the proceedings  
Institut professionnel des agents immobiliers (IPI)  
v  
Geoffrey Englebert,  
Immo 9 SPRL,  
Grégory Francotte,  
intervening parties:  
Union professionnelle nationale des détectives privés de Belgique (UPNDP),  
Association professionnelle des inspecteurs et experts d’assurances ASBL (APIEA),  
Conseil des ministres,  
THE COURT (Third Chamber),  
composed of M. Ilešič, President of the Chamber, C.G. Fernlund (Rapporteur), A. Ó Caoimh, C. Toader and E. Jarašiūnas, Judges,  
Advocate General: Y. Bot,  
Registrar: V. Tourrès, Administrator,  
having regard to the written procedure and further to the hearing on 11 July 2013,  
after considering the observations submitted on behalf of:  
–        Institut professionnel des agents immobiliers (IPI), by Y. Paquay and H. Nyssen, avocats,  
–        the Belgian Government, by M. Jacobs and C. Pochet, acting as Agents, and B. Renson, avocat,  
–        the Czech Government, by M. Smolek, acting as Agent,  
–        the Netherlands Government, by B. Koopman and C. Wissels, acting as Agents,  
–        the European Parliament, by A. Caiola and A. Pospíšilová Padowska, acting as Agents,  
–        the European Commission, by F. Clotuche-Duvieusart and B. Martenczuk, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 13(1)(d) and (g) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between the Institut professionnel des agents immobiliers (IPI) (Belgian Institute of Estate Agents) on the one hand and Mr Englebert, Immo 9 SPRL and Mr Francotte on the other concerning alleged breaches of the national rules on the exercise of the profession of estate agent.  
   
Legal context  
   
European Union law  
 Directive 95/46  
3        Recitals 3, 8, 10, 37 and 43 in the preamble to Directive 95/46 read as follows:  
‘(3)      Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;  
…   
(8)      Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; …  
…   
(10)      Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;  
…  
(37)      Whereas the processing of personal data for purposes of journalism or for purposes of literary [or] artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information …  
…  
(43)      Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; …’  
4        Article 1(1) of Directive 95/46 states:  
‘In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.’  
5        Article 2(a) and (d) of Directive 95/46 states:   
‘For the purpose of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); …  
…   
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; …’  
6        Article 9 of Directive 95/46 states:  
‘Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.’  
7        Section IV of Directive 95/46, entitled ‘Information to be given to the data subject’, comprises Articles 10 and 11 which govern situations where the data have been collected from the data subject and where the data have not been obtained from the data subject respectively.  
8        Article 10 of Directive 95/46 states:  
‘Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:  
(a)      the identity of the controller and of his representative, if any;  
(b)      the purposes of the processing for which the data are intended;  
(c)      any further information such as  
–        the recipients or categories of recipients,   
–        whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,   
–        the existence of the right of access to and the right to rectify the data concerning him  
in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.’  
9        Article 11 of the directive states that, where the data have not been obtained from the data subject, Member States are to provide that the controller or his representative must at the time of undertaking the recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the information set out in that article, except where he already has it.  
10      Paragraph 1 of Article 13 of Directive 95/46, which is entitled ‘Exemptions and restrictions’, provides:   
‘Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;  
(e)      an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;  
(f)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);  
(g)      the protection of the data subject or of the rights and freedoms of others.’  
 Directive 2002/58/EC  
11      Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37) provides in Article 15(1):  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. …’  
   
Belgian law  
12      The Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data (  
Moniteur belge  
, 18 March 1993, p. 5801) was amended by the Law of 11 December 1998 implementing Directive 95/46/EC (  
Moniteur belge  
, 3 February 1999, p. 3049) (‘the 1992 Law’). Article 9 of the 1992 Law, paragraphs 1 and 2 of which correspond to Articles 10 and 11 of the directive respectively, imposes an obligation to inform the data subject.  
13      Article 3(3) to (7) of the 1992 Law lays down exceptions and restrictions to that obligation to inform, inter alia, where the processing of personal data is carried out solely for journalistic purposes or the purpose of artistic or literary expression and where it is managed by the Sûreté de l’État (State security office), by the Service général du renseignement et de la sécurité (General intelligence and security service of the armed forces), by public authorities for the purpose of exercising their judicial police duties, by the police services for the purpose of exercising their administrative police duties, or by the European Centre for Missing and Sexually Abused Children.  
   
The facts in the main proceedings and the questions referred for a preliminary ruling  
14      IPI, established by Royal Decree of 17 February 1995, is, inter alia, responsible for ensuring compliance with the conditions of access to and the proper practice of the profession of estate agent. It may, for that purpose, be a party to legal proceedings and report to the judicial authorities any infringement of the applicable rules. IPI is authorised to use the services of private detectives in order to carry out its duties.  
15      In the course of its activity, IPI asked the Tribunal de commerce de Charleroi (Charleroi Commercial Court) to declare that Mr Englebert, Immo 9 SPRL and Mr Francotte had acted contrary to those rules and to order Mr Englebert and Mr Francotte to cease various estate agency activities. IPI based its action on facts gathered by private detectives whom it had used.  
16      The Tribunal de commerce de Charleroi raised the question of the value to be attributed to the evidence furnished by the private detectives, given the possibility that it had been obtained without respecting the requirements of the protection of individuals with regard to the processing of personal data and, consequently, in breach of the 1992 Law. That court stated that, according to IPI, the implementation of that law, which requires the data subject to be informed of the detective’s investigation in advance or, where the data is collected from third parties, at the time of undertaking the recording of the data at issue, makes it impossible for a private detective to carry on his activities. The Tribunal de commerce de Charleroi was uncertain whether, by not extending to private detectives the exceptions to that obligation to inform which apply to other professional categories or bodies working in the public interest, Article 3(3) to (7) of the 1992 Law gives rise to unequal treatment contrary to the Constitution. It therefore decided to refer the question to the Cour constitutionnelle (Constitutional Court).  
17      That court considers that it must be determined whether the 1992 Law, by not laying down exceptions for private detectives comparable to those referred to in Article 13(1)(d) and (g) of Directive 95/46, correctly implements that provision. It states that Article 3(3) to (7) of the 1992 Law gives rise to a difference in treatment between, on the one hand, persons pursuing a journalistic, artistic or literary activity, security and police services and the European Centre for Missing and Sexually Abused Children and, on the other, persons exercising the profession of private detective, in that only the former are exempt from the obligation to inform laid down in Article 9 of the 1992 Law.  
18      According to the referring court, that exception can be explained in terms of the activities exercised, which are related to public information or to cultural life, to the maintenance of security and public order, and to the defence of the fundamental rights of the most vulnerable.  
19      Private detectives are stated to be in a different situation. The referring court notes that, even though their profession is regulated by a 1991 law which establishes the structure of the profession and makes its exercise subject to the authorisation of the Minister for the Interior, their activity is unconnected with the protection of those fundamental rights and general interests and generally relates to the protection of private interests.  
20      The Cour constitutionnelle notes that, although Article 13(1) of Directive 95/46 seems to grant Member States some freedom as to whether or not to adopt the exceptions in question, nevertheless a doubt exists in view of the complete harmonisation achieved, in principle, by that directive.  
21      In those circumstances, the Cour constitutionnelle decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘1.      Is Article 13(1)(g)   
in fine   
of Directive [95/46] to be interpreted as meaning that it leaves the Member States free to choose whether or not to provide for an exception to the immediate obligation to inform set out in Article 11(1) if this is necessary in order to protect the rights and freedoms of others, or are the Member States subject to restrictions in this matter?  
2.      Do the professional activities of private detectives, governed by national law and exercised in the service of authorities authorised to report to the judicial authorities any infringement of the provisions protecting a professional title and organising a profession, come, depending on the circumstances, within the exception referred to in Article 13(1)(d) and (g)   
in fine  
 of [Directive 95/46]?  
3.      In the event of a negative reply to Question 2, is Article 13(1)(d) and (g)   
in fine  
 of [Directive 95/46] compatible with Article 6(3) [TEU], more specifically with the principle of equality and non-discrimination?’  
   
Consideration of the questions referred  
   
Preliminary observation  
22      In its first question, the referring court refers to an obligation to inform the data subject immediately which is referred to in Article 11 of Directive 95/46.  
23      It must, however, be observed that that provision, which concerns data which have not been obtained from the data subject, provides for information to be provided to the data subject not at the time when the data are obtained but at a later stage. By contrast, Article 10 of Directive 95/46, which refers to the collection of data from the data subject, provides for the data subject to be informed at the time the data are collected (see, to that effect, Case C-553/07   
Rijkeboer   
[2009] ECR I-3889, paragraph 68). The immediate nature of the provision of information to the data subject thus comes not from Article 11 of Directive 95/46, mentioned by the referring court, but from Article 10.  
24      As regards investigations carried out by a private detective, it is apparent from the order for reference that he may need to collect data either directly from the data subject or indirectly, inter alia, from third parties. It must, therefore, be stated that both Article 10 and Article 11(1) of Directive 95/46 may, depending on the circumstances, be relevant for such investigations.  
   
Questions 1 and 2  
25      By its first two questions, which should be considered together, the referring court asks, in essence, first, whether Article 13(1) of Directive 95/46 must be interpreted as meaning that Member States have the option, or the obligation, to transpose into their national law the exceptions which that article lays down to the obligation to inform data subjects of the processing of their personal data and, secondly, whether the activity of a private detective acting for a professional body in order to investigate breaches of ethics of a regulated profession, in this case that of estate agent, falls within the scope of Article 13(1)(d) or (g).  
26      At the outset, it must be stated that data such as those which, according to the referring court, are collected by the private detectives in the main proceedings relate to persons acting as estate agents and concern identified or identifiable natural persons. They are therefore personal data within the meaning of Article 2(a) of Directive 95/46. Their collection, storage and transmission by a regulated body such as IPI or by the private detectives acting for it therefore represent the ‘processing of personal data’ within the meaning of Article 2(b) of Directive 95/46 (see Case C-524/06   
Huber  
 [2008] ECR I-9705, paragraph 43).  
27      In order to reply to the question, it must be examined, in the first place, whether, pursuant to Article 13(1) of Directive 95/46, Member States have the option to provide, or are obliged to provide, for one or more of the exceptions listed in that article to the obligation to inform the data subject of the processing of personal data.  
28      It is apparent from recitals 3, 8 and 10 of Directive 95/46 that the European Union legislature sought to facilitate the free movement of personal data by the approximation of the laws of the Member States while safeguarding the fundamental rights of individuals, in particular the right to privacy, and ensuring a high level of protection in the European Union. Article 1 of the directive thus requires the Member States to ensure the protection of the fundamental rights and freedoms of natural persons, in particular their privacy, with respect to the processing of personal data (  
Huber  
, paragraph 47, and Joined Cases C-468/10 and C-469/10   
ASNEF and FECEMD  
 [2011] ECR I-12181, paragraph 25).  
29      For that purpose, Directive 95/46 contains, in Articles 10 and 11, obligations to inform the data subject of the processing of his personal data while providing, in Article 13(1), that the Member States may adopt legislative measures to restrict the scope of those obligations where such a measure is necessary for the purposes set out in Article 13(1)(a) to (g).  
30      The referring court raises the question of the leeway Member States have in view of the legislature’s objective of harmonisation, as set out in recital 8 of the directive, which is intended to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States.  
31      It should be noted that the Court has previously held that Directive 95/46 amounts to harmonisation which is generally complete (see Case C-101/01   
Lindqvist  
 [2003] ECR I-12971, paragraphs 95 and 96, and   
Huber  
, paragraphs 50 and 51). However, the Court has also found that the provisions of Directive 95/46 are necessarily relatively general given that it has to be applied to a large number of very different situations, and that the directive includes rules with a degree of flexibility and, in many instances, leaves to the Member States the task of deciding the details or choosing between options (  
Lindqvist  
, paragraph 83).  
32      As regards Article 13(1) of Directive 95/46, it is clear from its wording, and in particular from the use of the words ‘Member States may’, that that provision does not oblige the Member States to lay down in their national law exceptions for the purposes listed in Article 13(1)(a) to (g) but, on the contrary, the legislature intended to give them the freedom to decide whether, and if so for what purposes, they wish to take legislative measures aimed at limiting, inter alia, the extent of the obligations to inform the data subject. Furthermore, it is also apparent from the wording of Article 13(1) that the Member States may lay down such measures only when they are necessary. The requirement that the measures be ‘necessary’ is thus a precondition for the application of the option granted to Member States by Article 13(1), and does not mean that they are required to adopt the exceptions at issue in all cases where that condition is satisfied.  
33      That interpretation is, first, supported by the wording of recital 43 of Directive 95/46, according to which restrictions on the rights of information ‘may … be imposed by Member States in so far as they are necessary to safeguard’ those purposes. That interpretation is, next, confirmed by a comparison of, on the one hand, the wording of Article 13(1) of Directive 95/46 and, on the other hand, Article 9 and recital 37 of the directive, which for their part clearly impose an obligation on the Member States to provide for exceptions and derogations for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in so far as they are necessary to reconcile the right to privacy with the rules governing freedom of expression.  
34      That interpretation is also confirmed by the Court’s analysis in Case C-275/06   
Promusicae  
 [2008] ECR I-271 of Article 15(1) of the directive on privacy and electronic communications, which is formulated in similar terms to Article 13(1) of Directive 95/46 and, furthermore, expressly refers to that article.  
35      The Court found, first, that Article 15(1) gives Member States the possibility of providing for exceptions to the obligation of principle to ensure the confidentiality of personal data (  
Promusicae  
, paragraph 50).  
36      As regards one of those exceptions, the Court then held that Article 15(1) cannot, however, be interpreted as compelling the Member States, in the situations it sets out, to lay down an obligation to disclose (  
Promusicae  
, paragraphs 51 and 53).  
37      It must, therefore, be considered that Article 13(1) of Directive 95/46 offers Member States the option to provide for one or more of the exceptions that it sets out, but they are not compelled to do so.  
38      It must therefore be examined, in the second place, whether the activity of a private detective acting for a regulated body, such as IPI, falls within the scope of the exceptions provided for in Article 13(1)(d) and (g) of Directive 95/46.  
39      According to settled case-law, the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-73/07   
Satakunnan Markkinapörssi and Satamedia  
 [2008] ECR I-9831, paragraph 56, and Joined Cases C-92/09 and C-93/09   
Volker und Markus Schecke and Eifert  
 [2010] ECR I-11063, paragraphs 77 and 86).  
40      As regards the exceptions set out in Article 13(1)(d) and (g) of Directive 95/46, the former refers in particular to a specifically defined situation, namely the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, and the latter to the protection of the rights and freedoms of others, which by contrast are not defined.  
41      It is necessary first to examine the exception provided for in Article 13(1)(d) of the directive and ascertain whether it applies to the activity of a private detective acting for a body such as IPI.  
42      According to the order for reference, the profession of estate agent is a regulated profession in Belgium and IPI is a professional body responsible for ensuring compliance with the rules at issue through investigating and reporting breaches of those rules.  
43      The activity of a body such as IPI corresponds to the situation referred to by the exception in Article 13(1)(d) of Directive 95/46, and is therefore capable of coming under that exception.  
44      Since Directive 95/46 does not specify the manner in which the investigation and detection of failures to comply with the rules are carried out, it must be considered that the directive does not prevent such a professional body from having recourse to specialised investigators, such as private detectives responsible for that investigation and detection, in order to perform its duties.  
45      It follows that, if a Member State has chosen to implement the exception provided for in Article 13(1)(d), then the professional body concerned and the private detectives acting for it may rely on it and are not subject to the obligation to inform the data subject provided for in Articles 10 and 11 of Directive 95/46.  
46      If, on the other hand, the Member State has not provided for that exception, the data subjects must be informed of the processing of their personal data according to the detailed provisions, in particular those concerning timing, of Articles 10 and 11.  
47      According to IPI, application of the exception to the obligation to inform, to IPI itself and to private detectives acting on its behalf, is necessary for it to carry out its role. The IPI claims it would be impossible for private detectives to carry out their activity for IPI effectively if they had to disclose their identity and the reasons for their investigations before even questioning the persons they are investigating. The Netherlands Government also claimed that the investigations at issue would be bound to fail.  
48      As is apparent from paragraph 37 above, however, it is for the Member States to decide whether they consider it necessary to provide, in their legislation for the exception laid down in Article 13(1)(d) of Directive 95/46 in favour of professional bodies such as IPI, acting directly or with the help of private detectives. It is open to them to take the view that those professional bodies and the private detectives acting for them have sufficient means, notwithstanding the application of Articles 10 and 11 of that directive, of detecting the breaches of ethics at issue, so that it is not necessary for that exception to be implemented in order for those bodies to be able to carry out their duty of ensuring compliance with the rules.  
49      As to the extent of that exception, the concept of ‘breaches of ethics’ must next be defined. Differences in opinion have emerged in the written and oral observations submitted to the Court on this point. According to the Belgian Government, and contrary to what IPI claims, the breaches in question only concern the conduct of estate agents duly licenced to practise their profession and do not extend to the conduct of persons who, without being licensed, pass themselves off as estate agents.  
50      In that regard, it should be stated that the rules on access to a regulated profession form part of the rules of professional ethics. It follows that investigations concerning the acts of persons who breach those rules by passing themselves off as estate agents are covered by the exception in Article 13(1)(d) of Directive 95/46.  
51      Consequently, under that directive, Member States may provide that a regulated professional body, such as IPI, may, alone or with the help of private detectives, investigate possible breaches of the rules of ethics, including breaches resulting from the acts of persons who have failed to observe the rules relating to access to the profession, while being covered by that exception.  
52      Having regard to the scope of that exception, it is not necessary to examine whether the activity of a private detective acting for a professional body such as IPI is also covered by the exception provided for in Article 13(1)(g) of Directive 95/46.  
53      The answer to the first two questions is therefore that:  
–        Article 13(1) of Directive 95/46 must be interpreted as meaning that Member States have no obligation, but have the option, to transpose into their national law one or more of the exceptions which it lays down to the obligation to inform data subjects of the processing of their personal data;  
–        the activity of a private detective acting for a professional body in order to investigate breaches of ethics of a regulated profession, in this case that of estate agent, is covered by the exception in Article 13(1)(d) of Directive 95/46.  
   
Question 3  
54      Given the answer to the first two questions, there is no need to answer the third question.  
   
Costs  
55      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.   
On those grounds, the Court (Third Chamber) hereby rules:  
Article 13(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that Member States have no obligation, but have the option, to transpose into their national law one or more of the exceptions which it lays down to the obligation to inform data subjects of the processing of their personal data.  
The activity of a private detective acting for a professional body in order to investigate breaches of ethics of a regulated profession, in this case that of estate agent, is covered by the exception in Article 13(1)(d) of Directive 95/46.

ID: af8f4140-78a8-4002-b3ce-07088e440932

of 4 Jul 2023, C-252/21 (  
Meta Platforms and Others  
)  
   
JUDGMENT OF THE COURT (Grand Chamber)  
4 July 2023 (\*)  
Table of contents  
Legal context  
European Union law  
Regulation No 1/2003  
The GDPR  
German law  
The dispute in the main proceedings and the questions referred for a preliminary ruling  
The questions referred  
Questions 1 and 7  
Question 2  
Question 2(a)  
Question 2(b)  
Questions 3 to 5  
Preliminary observations  
Questions 3 and 4  
Question 5  
Question 6  
Costs  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Social networks – Abuse of a dominant position by the operator of such a network – Abuse which entails the processing of the personal data of the users of that network as provided for in its general terms of use – Powers of a competition authority of a Member State to find that processing is not consistent with that regulation – Reconciliation with the powers of the national data protection supervisory authorities – Article 4(3) TEU – Principle of sincere cooperation – Points (a) to (f) of the first subparagraph of Article 6(1) of Regulation 2016/679 – Whether the processing is lawful – Article 9(1) and (2) – Processing of special categories of personal data – Article 4(11) – Concept of ‘consent’)  
In Case C-252/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany), made by decision of 24 March 2021, received at the Court on 22 April 2021, in the proceedings  
Meta Platforms Inc.,  
 formerly Facebook Inc.,  
Meta Platforms Ireland Ltd,  
 formerly Facebook Ireland Ltd,  
Facebook Deutschland GmbH  
v  
Bundeskartellamt,  
intervener:  
Verbraucherzentrale Bundesverband eV,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Prechal, K. Jürimäe, C. Lycourgos, M. Safjan, L.S. Rossi (Rapporteur), D. Gratsias and M.L. Arastey Sahún, Presidents of Chambers, J.-C. Bonichot, S. Rodin, F. Biltgen, M. Gavalec, Z. Csehi and O. Spineanu-Matei, Judges,  
Advocate General: A. Rantos,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 10 May 2022,  
after considering the observations submitted on behalf of:  
–        Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, and Facebook Deutschland GmbH, by M. Braun, M. Esser, L. Hesse, J. Höft and H.-G. Kamann, Rechtsanwälte,  
–        the Bundeskartellamt, by J. Nothdurft, K. Ost, I. Sewczyk and J. Topel, acting as Agents,  
–        Verbraucherzentrale Bundesverband eV, by S. Louven, Rechtsanwalt,  
–        the German Government, by J. Möller and P.-L. Krüger, acting as Agents,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and E. De Bonis and P. Gentili, avvocati dello Stato,  
–        the Austrian Government, by A. Posch, J. Schmoll and G. Kunnert, acting as Agents,  
–        the European Commission, by F. Erlbacher, H. Kranenborg and G. Meessen, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 20 September 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 4(3) TEU and of Article 6(1), Article 9(1) and (2), Article 51(1) and Article 56(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2; ‘the GDPR’).  
2        The request has been made in proceedings between Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, and Facebook Deutschland GmbH, on the one hand, and the Bundeskartellamt (Federal Cartel Office, Germany), on the other, concerning the decision by which the latter prohibited those companies from processing certain personal data as provided for in the general terms of use of the social network Facebook (‘the general terms’).  
   
Legal context  
   
European Union law  
   
Regulation (EC) No 1/2003  
3        Article 5 of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles [101 and 102 TFEU] (OJ 2003 L 1, p. 1), entitled ‘Powers of the competition authorities of the Member States’, provides:  
‘The competition authorities of the Member States shall have the power to apply Articles [101 and 102 TFEU] in individual cases. For this purpose, acting on their own initiative or on a complaint, they may take the following decisions:  
–        requiring that an infringement be brought to an end,  
–        ordering interim measures,  
–        accepting commitments,  
–        imposing fines, periodic penalty payments or any other penalty provided for in their national law.  
Where on the basis of the information in their possession the conditions for prohibition are not met they may likewise decide that there are no grounds for action on their part.’  
   
The GDPR  
4        Recitals 1, 4, 38, 42, 43, 46, 47, 49 and 51 of the GDPR state:  
‘(1)      The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the “Charter”) and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.  
…  
(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.  
…  
(38)      Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.  
…  
(42)      Where processing is based on the data subject’s consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. … For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.  
(43)      In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.  
…  
(46)      The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.  
(47)      The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. … At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. … The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.  
…  
(49)      The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems … constitutes a legitimate interest of the data controller concerned. …  
…  
(51)      Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term “racial origin” in this Regulation does not imply an acceptance by the [European] Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.’  
5        Article 4 of that regulation provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); …  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;  
…  
(11)      “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;  
…  
(23)      “cross-border processing” means either:  
(a)      processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or  
(b)      processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.  
…’  
6        Article 5 of that regulation, headed ‘Principles relating to processing of personal data’, provides:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; …  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
…  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
7        Article 6 of the regulation, entitled ‘Lawfulness of processing’, reads as follows:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
(d)      processing is necessary in order to protect the vital interests of the data subject or of another natural person;  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.  
…  
3.      The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:  
(a)      Union law; or  
(b)      Member State law to which the controller is subject.  
…  
… The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.’  
8        Article 7 of the GDPR, entitled ‘Conditions for consent’, states:  
‘1.      Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.  
…  
4.      When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.’  
9        Article 9 of that regulation, entitled ‘Processing of special categories of personal data’, provides:  
‘1.      Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.  
2.      Paragraph 1 shall not apply if one of the following applies:  
(a)      the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law [provides] that the prohibition referred to in paragraph 1 may not be lifted by the data subject;  
…  
(e)      processing relates to personal data which are manifestly made public by the data subject;  
(f)      processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;  
…’  
10      Article 13 of that regulation, ‘Information to be provided where personal data are collected from the data subject’, provides, in its paragraph 1, as follows:  
‘Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:  
…  
(c)      the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;  
(d)      where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;  
…’  
11      Chapter VI of the GDPR, ‘Independent supervisory authorities’, comprises Articles 51 to 59 of the regulation.  
12      Under Article 51(1) and (2) of the GDPR, that article being entitled ‘Supervisory authority’:  
‘1.      Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union …  
2.      Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the [European] Commission in accordance with Chapter VII.’  
13      As set out in Article 55 of the GDPR, headed ‘Competence’:  
‘1.      Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.  
2.      Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.’  
14      Article 56(1) of that regulation, that article being entitled ‘Competence of the lead supervisory authority’, states:  
‘Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.’  
15      Article 57(1) of that regulation, that article being entitled ‘Tasks’, provides:  
‘Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:  
(a)      monitor and enforce the application of this Regulation;  
…  
(g)      cooperate with, including sharing information[,] and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;  
…’  
16      Article 58 of the regulation lists, in paragraph 1, the investigative powers available to each supervisory authority and states, in paragraph 5, that ‘each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation’.  
17      Section 1, entitled ‘Cooperation’, of Chapter VII of the GDPR comprises Articles 60 to 62 of that regulation. Article 60, ‘Cooperation between the lead supervisory authority and the other supervisory authorities concerned’, provides in paragraph 1:  
‘The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.’  
18      Article 61(1) of the GDPR, that article being headed ‘Mutual assistance’, states:  
‘Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.’  
19      Article 62 of that regulation, headed ‘Joint operations of supervisory authorities’, provides in paragraphs 1 and 2:  
‘1.      The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.  
2.      Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. …’  
20      Section 2, entitled ‘Consistency’, of Chapter VII of the GDPR comprises Articles 63 to 67 of that regulation. Article 63, headed ‘Consistency mechanism’, is worded as follows:  
‘In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.’  
21      Article 64(2) of that regulation is worded as follows:  
‘Any supervisory authority, the Chair of the [European Data Protection] Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the [European Data Protection] Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.’  
22      Article 65(1) of that regulation, that article being headed ‘Dispute resolution by the Board’, provides:  
‘In order to ensure the correct and consistent application of this Regulation in individual cases, the [European Data Protection] Board shall adopt a binding decision in the following cases:  
(a)      where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;  
(b)      where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;  
…’  
   
German law  
23      Paragraph 19(1) of the Gesetz gegen Wettbewerbsbeschränkungen (Law against restrictions on competition), in its version published on 26 June 2013 (BGBl. 2013 I, p. 1750, 3245), last amended by Paragraph 2 of the Law of 16 July 2021 (BGBl. 2021 I, p. 2959) (‘the GWB’), provides:  
‘The abuse of a dominant position by one or more undertakings is prohibited.’  
24      In accordance with Paragraph 32(1) of the GWB:  
‘The competition authority may require undertakings or associations of undertakings to bring to an end an infringement of a provision of this Part or of Articles 101 or 102 [TFEU].’  
25      Paragraph 50f(1) of the GWB provides:  
‘The competition authorities, the regulatory authorities, the federal data protection and freedom of information officer, the regional data protection officers and the competent authorities within the meaning of Paragraph 2 of the EU-Verbraucherschutzdurchführungsgesetz [(Law on the implementation of EU consumer protection law)] may, irrespective of the procedure chosen, exchange information, including personal data and trade and business secrets, to the extent necessary for the performance of their respective tasks and may use that information in the course of their proceedings. …’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
26      Meta Platforms Ireland operates the online social network Facebook within the European Union and promotes, inter alia via www.facebook.com, services that are free of charge for private users. Other undertakings of the Meta group offer, within the European Union, other online services, including Instagram, WhatsApp, Oculus and – until 13 March 2020 – Masquerade.  
27      The business model of the online social network Facebook is based on financing through online advertising, which is tailored to the individual users of the social network according, inter alia, to their consumer behaviour, interests, purchasing power and personal situation. Such advertising is made possible in technical terms by the automated production of detailed profiles in respect of the network users and the users of the online services offered at the level of the Meta group. To that end, in addition to the data provided by the users directly when they sign up for the online services concerned, other user- and device-related data are also collected on and off that social network and the online services provided by the Meta group, and linked to their various user accounts. The aggregate view of the data allows detailed conclusions to be drawn about those users’ preferences and interests.  
28      For the processing of those data, Meta Platforms Ireland relies on the user agreement to which the users of the social network Facebook adhere when they click on the ‘Sign up’ button, thereby accepting the general terms drawn up by that company. Acceptance of those terms is necessary in order to be able to use the social network Facebook. With regard to the processing of personal data, the general terms refer to that company’s data and cookies policies. According to those policies, Meta Platforms Ireland collects user- and device-related data about user activities on and off the social network and links the data with the Facebook accounts of the users concerned. The latter data, relating to activities outside the social network (‘the off-Facebook data’), are data concerning visits to third-party webpages and apps, which are linked to Facebook through programming interfaces – ‘Facebook Business Tools’ – as well as data concerning the use of other online services belonging to the Meta group, including Instagram, WhatsApp, Oculus and – until 13 March 2020 – Masquerade.  
29      The Federal Cartel Office brought proceedings against Meta Platforms, Meta Platforms Ireland and Facebook Deutschland, as a result of which, by decision of 6 February 2019, based on Paragraph 19(1) and Paragraph 32 of the GWB, it essentially prohibited those companies from making, in the general terms, the use of the social network Facebook by private users resident in Germany subject to the processing of their off-Facebook data and from processing the data without their consent on the basis of the general terms in force at the time. In addition, it required them to adapt those general terms in such a way that it is made clear that those data will neither be collected, nor linked with Facebook user accounts nor used without the consent of the user concerned, and it clarified the fact that such a consent is not valid if it is a condition for using the social network.  
30      The Federal Cartel Office based its decision on the fact that the processing of the data of the users concerned, as provided for in the general terms and implemented by Meta Platforms Ireland, constituted an abuse of that company’s dominant position on the market for online social networks for private users in Germany, within the meaning of Paragraph 19(1) of the GWB. In particular, according to the Federal Cartel Office, those general terms, as a result of that dominant position, constitute an abuse since the processing of the off-Facebook data that they provide for is not consistent with the underlying values of the GDPR and, in particular, it cannot be justified in the light of Article 6(1) and Article 9(2) of that regulation.  
31      On 11 February 2019, Meta Platforms, Meta Platforms Ireland and Facebook Deutschland brought an action against the decision of the Federal Cartel Office before the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany).  
32      On 31 July 2019, Meta Platforms Ireland introduced new general terms expressly stating that the user, instead of paying to use Facebook products, agrees to being shown advertisements.  
33      Furthermore, since 28 January 2020, Meta Platforms has been offering, at a global level, ‘  
Off-Facebook Activity  
’, which allows the users of the social network Facebook to view a summary of the information about them that Meta group companies obtain in relation to their activities on other websites and apps, and to disconnect the data about past and future activities from their Facebook.com account if they so wish.  
34      The Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf) has doubts (i) as to whether national competition authorities may review, in the exercise of their powers, whether the processing of personal data complies with the requirements set out in the GDPR; (ii) as to whether the operator of an online social network may process the data subject’s sensitive personal data within the meaning of Article 9(1) and (2) of that regulation; (iii) as to the lawfulness of the processing by such an operator of the personal data of the user concerned, under Article 6(1) of that regulation; and (iv) as to the validity, in the light of point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of that regulation, of the consent given to an undertaking with a dominant position on the national market for online social networks for the purposes of such processing.  
35      In those circumstances, taking the view that the resolution of the case in the main proceedings depends on the answer to those questions, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      (a)      Is it compatible with Article 51 et seq. of the GDPR if a national competition authority – such as the … Federal Cartel Office – which is not a supervisory authority within the meaning of Article 51 et seq. of the GDPR, of a Member State in which an undertaking established outside the European Union has an establishment that provides the main establishment of that undertaking – which is located in another Member State and has sole responsibility for processing personal data for the entire territory of the European Union – with advertising, communication and public relations support, finds, for the purposes of monitoring abuses of competition law, that the main establishment’s contractual terms relating to data processing and their implementation breach the GDPR and issues an order to end that breach?  
(b)      If so: is that compatible with Article 4(3) TEU if, at the same time, the lead supervisory authority in the Member State in which the main establishment, within the meaning of Article 56(1) of the GDPR, is located is investigating the undertaking’s contractual terms relating to data processing?  
If the answer to Question 1 is “yes”:  
(2)      (a)      If an internet user merely visits websites or apps to which the criteria of Article 9(1) of the GDPR relate, such as flirting apps, gay dating sites, political party websites or health-related websites, or also enters information into them, for example when registering or when placing orders, and [an] undertaking, such as [Meta Platforms   
   
Ireland], uses interfaces integrated into those websites and apps, such as “Facebook Business Tools”, or cookies or similar storage technologies placed on the internet user’s computer or mobile device, to collect data about those visits to the websites and apps and the information entered by the user, and links those data with the data from the user’s Facebook  
.  
com account and uses them, does this collection and/or linking and/or use involve the processing of sensitive data for the purpose of that provision?  
(b)      If so: does visiting those websites or apps and/or entering information and/or clicking or tapping on the buttons integrated into them by a provider such as [Meta Platforms   
   
Ireland] (social plugins such as “Like”, “Share” or “Facebook Login” or “Account Kit”) constitute manifestly making the data about the visits themselves and/or the information entered by the user public within the meaning of Article 9(2)(e) of the GDPR?  
(3)      Can an undertaking, such as [Meta Platforms   
   
Ireland], which operates a digital social network funded by advertising and offers personalised content and advertising, network security, product improvement and consistent, seamless use of all of its group products in its terms of service, justify collecting data for these purposes from other group services and third-party websites and apps via integrated interfaces such as “Facebook Business Tools”, or via cookies or similar storage technologies placed on the internet user’s computer or mobile device, linking those data with the user’s Facebook.com account and using them, on the ground of necessity for the performance of the contract under Article 6(1)(b) of the GDPR or on the ground of the pursuit of legitimate interests under Article 6(1)(f) of the GDPR?  
(4)      In those circumstances, can  
–        the fact of users being underage, vis-à-vis the personalisation of content and advertising, product improvement, network security and non-marketing communications intended for the user;  
–        the provision of measurements, analytics and other business services to enable advertisers, developers and other partners to evaluate and improve their services;  
–        the provision of marketing communications intended for the user to enable the undertaking to improve its products and engage in direct marketing;  
–        research and innovation for social good, to further the state of the art or the academic understanding of important social issues and to affect society and the world in a positive way;  
–        the sharing of information with law-enforcement agencies and responding to legal requests in order to prevent, detect and prosecute criminal offences, unlawful use, breaches of the terms of service and policies and other harmful behaviour;  
also constitute legitimate interests within the meaning of Article 6(1)(f) of the GDPR if, for those purposes, the undertaking [collects data from other group services and from third-party websites and apps via integrated interfaces such as “Facebook Business Tools”, or via cookies or similar storage technologies placed on the internet user’s computer or mobile device, links those data with the user’s Facebook.com account and uses them]?  
(5)      In those circumstances, can collecting data from other group services and from third-party websites and apps via integrated interfaces such as “Facebook Business Tools”, or via cookies or similar storage technologies placed on the internet user’s computer or mobile device, linking those data with the user’s Facebook.com account and using them, or using data already collected and linked by other lawful means, also be justified under Article 6(1)(c), (d) and (e) of the GDPR in individual cases, for example to respond to a legitimate request for certain data (point (c)), to combat harmful behaviour and promote security (point (d)), to research for social good and to promote safety, integrity and security (point (e))?  
(6)      Can consent within the meaning of Article 6(1)(a) and Article 9(2)(a) of the GDPR be given effectively and, in accordance with Article 4(11) of the GDPR in particular, freely, to a dominant undertaking such as [Meta Platforms   
   
Ireland]?  
If the answer to Question 1 is “no”:  
(7)      (a)      Can the national competition authority of a Member State, such as the Federal Cartel Office, which is not a supervisory authority within the meaning of Article 51 et seq. of the GDPR and which examines a breach by a dominant undertaking of the competition-law prohibition on abuse that is not a breach of the GDPR by that undertaking’s data processing terms and their implementation, make findings, when assessing the balance of interests, as to whether those data processing terms and their implementation comply with the GDPR?  
(b)      If so: in the light of Article 4(3) TEU, does that also apply if the competent lead supervisory authority in accordance with Article 56(1) of the GDPR is investigating the undertaking’s data processing terms at the same time?  
If the answer to Question 7 is “yes”, Questions 3 to 5 must be answered in relation to data from the use of the group’s Instagram service.’  
   
The questions referred  
   
Questions 1 and 7  
36      By Questions 1 and 7, which it is appropriate to examine together, the referring court asks, in essence, whether Article 51 et seq. of the GDPR must be interpreted as meaning that a competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position by an undertaking within the meaning of Article 102 TFEU, that that undertaking’s general terms of use relating to the processing of personal data and the implementation thereof are not consistent with the GDPR, and if so, whether Article 4(3) TEU must be interpreted as meaning that such a finding, of an incidental nature, by the competition authority is also possible where those terms are being investigated, simultaneously, by the competent lead supervisory authority in accordance with Article 56(1) of the GDPR.  
37      In order to answer that question, it is important to recall at the outset that Article 55(1) of the GDPR states the general rule that each supervisory authority is to be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it, in accordance with that regulation, on the territory of its own Member State (judgment of 15 June 2021,   
Facebook Ireland and Others  
, C-645/19, EU:C:2021:483, paragraph 47 and the case-law cited).  
38      The tasks assigned to those supervisory authorities include monitoring and enforcing the application of the GDPR, as provided for in Article 51(1) and Article 57(1)(a) of that regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of such data within the European Union. In addition, in accordance with Article 51(2) and Article 57(1)(g) of that regulation, the supervisory authorities must cooperate with each other, including sharing information, and provide mutual assistance with a view to ensuring the consistency of application and enforcement of the regulation.  
39      In order to carry out those tasks, Article 58 of the GDPR confers on those supervisory authorities, in paragraph 1, investigative powers, in paragraph 2, corrective powers, and in paragraph 5, the power to bring infringements of that regulation to the attention of the judicial authorities and, where appropriate, to commence legal proceedings in order to enforce the provisions of that regulation.  
40      Without prejudice to the rule on competence set out in Article 55(1) of the GDPR, Article 56(1) of that regulation lays down, with respect to ‘cross-border processing’, within the meaning of Article 4(23) of that regulation, the ‘one-stop-shop mechanism’, based on an allocation of competences between one ‘lead supervisory authority’ and the other supervisory authorities concerned as well as on cooperation between all of those authorities in accordance with the cooperation procedure laid down in Article 60 of that regulation.  
41      Furthermore, Article 61(1) of the GDPR obliges the supervisory authorities, inter alia, to provide each other with relevant information and mutual assistance in order to implement and apply that regulation in a consistent manner throughout the European Union. Article 63 of the GDPR states that it was for that purpose that provision was made for the consistency mechanism set out in Articles 64 and 65 of that regulation (judgment of 15 June 2021,   
Facebook Ireland and Others  
, C-645/19, EU:C:2021:483, paragraph 52 and the case-law cited).  
42      That said, it should be noted that the rules on cooperation laid down in the GDPR are not addressed to the national competition authorities but govern cooperation between the national supervisory authorities concerned and the lead supervisory authority as well as, where appropriate, cooperation between those authorities and the European Data Protection Board and the Commission.  
43      Neither the GDPR nor any other instrument of EU law provides for specific rules on cooperation between a national competition authority and the relevant national supervisory authorities concerned or the lead supervisory authority. Furthermore, there is no provision in that regulation that prevents the national competition authorities from finding, in the performance of their duties, that a data processing operation carried out by an undertaking in a dominant position and liable to constitute an abuse of that position does not comply with that regulation.  
44      In that regard, it should be made clear, in the first place, that the supervisory authorities, on the one hand, and the national competition authorities, on the other, perform different functions and pursue their own objectives and tasks.  
45      On the one hand, as has been stated in paragraph 38 above, under Article 51(1) and (2) and Article 57(1)(a) and (g) of the GDPR, the primary task of the supervisory authority is to monitor and enforce the application of that regulation, while contributing to its consistent application within the European Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of such data within the European Union. To that end, as recalled in paragraph 39 above, the supervisory authority has at its disposal the various powers conferred on it under Article 58 of the GDPR.  
46      On the other hand, in accordance with Article 5 of Regulation No 1/2003, the national competition authorities have the power to take, inter alia, decisions finding an abuse of a dominant position by an undertaking, within the meaning of Article 102 TFEU, whose objective is to establish a system which ensures that competition in the internal market is not distorted, having regard also to the consequences of such an abuse for consumers in that market.  
47      As the Advocate General observed, in essence, in point 23 of his Opinion, when taking such a decision, a competition authority must assess, on the basis of all the specific circumstances of the case, whether, by resorting to methods different from those governing normal competition in products or services, the conduct of the dominant undertaking has the effect of hindering the maintenance of the degree of competition existing in the market or the growth of that competition (see, to that effect, judgment of 25 March 2021,   
Deutsche Telekom  
 v   
Commission  
, C-152/19 P, EU:C:2021:238, paragraphs 41 and 42). In that respect, the compliance or non-compliance of that conduct with the provisions of the GDPR may, depending on the circumstances, be a vital clue among the relevant circumstances of the case in order to establish whether that conduct entails resorting to methods governing normal competition and to assess the consequences of a certain practice in the market or for consumers.  
48      It follows that, in the context of the examination of an abuse of a dominant position by an undertaking on a particular market, it may be necessary for the competition authority of the Member State concerned also to examine whether that undertaking’s conduct complies with rules other than those relating to competition law, such as the rules on the protection of personal data laid down by the GDPR.  
49      In view of the different objectives pursued by the rules established in competition matters, in particular Article 102 TFEU, on the one hand, and those laid down in relation to the protection of personal data under the GDPR, on the other, it must be held that, where a national competition authority identifies an infringement of that regulation in the context of the finding of an abuse of a dominant position, it does not replace the supervisory authorities. In particular, that national competition authority neither monitors nor enforces the application of that regulation for the purpose referred to in Article 51(1) of the GDPR, namely in order to protect the fundamental rights and freedoms of natural persons in relation to processing or to facilitate the free flow of personal data within the European Union. Furthermore, by merely noting the non-compliance of a data processing operation with the GDPR for the sole purpose of establishing an abuse of a dominant position and by imposing measures to put an end to that abuse on a legal basis derived from competition law, that authority does not carry out any of the tasks set out in Article 57 of that regulation, nor does it make use of the powers reserved to the supervisory authority under Article 58 of that regulation.  
50      Moreover, it is important to state that access to and use of personal data are of great importance in the context of the digital economy. That importance is illustrated, in the context of the dispute in the main proceedings, by the business model on which the social network Facebook relies, which, as recalled in paragraph 27 above, provides for financing through the marketing of personalised advertising messages according to user profiles established on the basis of personal data collected by Meta Platforms Ireland.  
51      As pointed out by the Commission, inter alia, access to personal data and the fact that it is possible to process such data have become a significant parameter of competition between undertakings in the digital economy. Therefore, excluding the rules on the protection of personal data from the legal framework to be taken into consideration by the competition authorities when examining an abuse of a dominant position would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union.  
52      However, in the second place, it should be noted that, where a national competition authority considers it necessary to rule, in the context of a decision on an abuse of a dominant position, on the compliance or non-compliance with the GDPR of the processing of personal data by the undertaking in question, that authority and the supervisory authority concerned or, where appropriate, the competent lead supervisory authority within the meaning of that regulation must cooperate with each other in order to ensure the consistency of application of that regulation.  
53      Although, as has been noted in paragraphs 42 and 43 above, neither the GDPR nor any other instrument of EU law provides for specific rules in that regard, the fact remains that, as the Advocate General observed, in essence, in point 28 of his Opinion, when they apply the GDPR, the various national authorities involved are all bound by the duty of sincere cooperation enshrined in Article 4(3) TEU. Under that principle, in accordance with settled case-law, in areas covered by EU law, Member States, including their administrative authorities, must assist each other, in full mutual respect, in carrying out tasks which flow from the Treaties, take any appropriate measure to ensure fulfilment of the obligations arising from, inter alia, the acts of the institutions of the European Union and refrain from any measure which could jeopardise the attainment of the European Union’s objectives (see, to that effect, judgments of 7 November 2013,   
UPC Nederland  
, C-158/11, EU:C:2013:709, paragraph 59, and of 1 August 2022,   
Sea Watch  
, C-14/21 and C-15/21, EU:C:2022:604, paragraph 156).  
54      Thus, in the light of this principle, when national competition authorities are called upon, in the exercise of their powers, to examine whether an undertaking’s conduct is consistent with the provisions of the GDPR, they are required to consult and cooperate sincerely with the national supervisory authorities concerned or with the lead supervisory authority, all of which are then bound, in that context, to observe their respective powers and competences, in such a way as to ensure that the obligations arising from the GDPR and the objectives of that regulation are complied with while their effectiveness is safeguarded.  
55      The examination by a competition authority of an undertaking’s conduct in the light of the provisions of the GDPR may entail the risk of divergences between that authority and the supervisory authorities in the interpretation of that regulation.  
56      It follows that, where, in the context of the examination seeking to establish whether there is an abuse of a dominant position within the meaning of Article 102 TFEU by an undertaking, a national competition authority takes the view that it is necessary to examine whether that undertaking’s conduct is consistent with the provisions of the GDPR, that authority must ascertain whether that conduct or similar conduct has already been the subject of a decision by the competent national supervisory authority or the lead supervisory authority or the Court. If that is the case, the national competition authority cannot depart from it, although it remains free to draw its own conclusions from the point of view of the application of competition law.  
57      Where it has doubts as to the scope of the assessment carried out by the competent national supervisory authority or the lead supervisory authority, where the conduct in question or similar conduct is, simultaneously, under examination by those authorities, or where, in the absence of investigation by those authorities, it takes the view that an undertaking’s conduct is not consistent with the provisions of the GDPR, the national competition authority must consult and seek their cooperation in order to dispel its doubts or to determine whether it must wait for the supervisory authority concerned to take a decision before starting its own assessment.  
58      For its part, where the supervisory authority is called upon by a national competition authority, it must respond to such a request for information or cooperation within a reasonable period of time, providing the latter with the information in its possession capable of dispelling that authority’s doubts as to the scope of the assessment carried out by the supervisory authority or, where appropriate, by informing the national competition authority if it intends to initiate the cooperation procedure with the other supervisory authorities concerned or with the lead supervisory authority, in accordance with Article 60 et seq. of the GDPR, in order to reach a decision seeking to establish whether or not the conduct in question is consistent with that regulation.  
59      In the absence of a reply, within a reasonable time, from the supervisory authority thus called upon, the national competition authority may continue its own investigation. The same applies where the competent national supervisory authority and the lead supervisory authority have no objection to such an investigation being continued without having to wait for a decision on their part.  
60      In the present case, it is apparent from the file before the Court that in October and November 2018, that is to say, before the adoption of the decision of 6 February 2019, the Federal Cartel Office contacted the Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (Federal Commissioner for Data Protection and Freedom of Information, Germany), the Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Commissioner for Data Protection and Freedom of Information, Hamburg, Germany), which is the competent authority for Facebook Deutschland, and the Data Protection Commission (DPC) (Ireland), to notify those authorities of the action it had taken. In addition, it is apparent that the Federal Cartel Office obtained confirmation that no investigation was being conducted at the time by those authorities in relation to facts similar to those at issue in the main proceedings, and they raised no objection to its actions. Finally, in paragraphs 555 and 556 of its decision of 6 February 2019, the Federal Cartel Office expressly referred to that cooperation.  
61      In those circumstances, and subject to verification by the referring court, the Federal Cartel Office appears to have fulfilled its obligations of sincere cooperation with the national supervisory authorities concerned and the lead supervisory authority.  
62      In the light of the foregoing, the answer to Questions 1 and 7 is that Article 51 et seq. of the GDPR and Article 4(3) TEU must be interpreted as meaning that, subject to compliance with its duty of sincere cooperation with the supervisory authorities, a competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position by an undertaking within the meaning of Article 102 TFEU, that that undertaking’s general terms of use relating to the processing of personal data and the implementation thereof are not consistent with that regulation, where that finding is necessary to establish the existence of such an abuse.  
63      In view of this duty of sincere cooperation, the national competition authority cannot depart from a decision by the competent national supervisory authority or the competent lead supervisory authority concerning those general terms or similar general terms. Where it has doubts as to the scope of such a decision, where those terms or similar terms are, simultaneously, under examination by those authorities, or where, in the absence of an investigation or decision by those authorities, the competition authority takes the view that the terms in question are not consistent with the GDPR, it must consult and seek the cooperation of those supervisory authorities in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment. In the absence of any objection on their part or of any reply within a reasonable time, the national competition authority may continue its own investigation.  
   
Q  
uestion  
 2  
64      By Question 2(a), the referring court asks, in essence, whether Article 9(1) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories referred to in that provision relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user’s social network account and the use of those data by that operator, must be regarded as ‘processing of special categories of personal data’ within the meaning of that provision, which is in principle prohibited, subject to the derogations provided for in Article 9(2).  
65      If so, the referring court asks, in essence, by Question 2(b), whether Article 9(2)(e) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which the categories set out in Article 9(1) of the GDPR relate, enters information into those sites or apps or clicks or taps on the buttons integrated into them, such as the ‘Like’ or ‘Share’ buttons or the buttons enabling the user to identify himself or herself on those sites or apps using the login credentials linked to his or her online social network user account, his or her telephone number or email address, the user is deemed to have manifestly made public, within the meaning of the first of those provisions, the data collected on that occasion by the operator of that online social network via cookies or similar storage technologies.  
   
Question 2(a)  
66      Recital 51 of the GDPR states that personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. That recital further states that such personal data should not be processed unless processing is allowed in the specific cases set out in that regulation.  
67      In that context, Article 9(1) of the GDPR lays down the principle that the processing of special categories of personal data listed therein is prohibited. This includes data revealing racial or ethnic origin, political opinions, religious beliefs and data concerning health or a natural person’s sex life or sexual orientation.  
68      For the purposes of applying Article 9(1) of the GDPR, it is important to determine, where personal data is processed by the operator of an online social network, if those data allow information falling within one of the categories referred to in that provision to be revealed, irrespective of whether that information concerns a user of that network or any other natural person. If so, then such processing of personal data is prohibited, subject to the derogations provided for in Article 9(2) of the GDPR.  
69      As the Advocate General observed, in essence, in points 40 and 41 of his Opinion, that fundamental prohibition, laid down in Article 9(1) of the GDPR, is independent of whether or not the information revealed by the processing operation in question is correct and of whether the controller is acting with the aim of obtaining information that falls within one of the special categories referred to in that provision.  
70      In view of the significant risks to the fundamental freedoms and fundamental rights of data subjects arising from any processing of personal data falling within the categories referred to in Article 9(1) of the GDPR, the objective thereof is to prohibit such processing, irrespective of its stated purpose.  
71      In the present case, the processing operation at issue in the main proceedings carried out by Meta Platforms Ireland entails, first of all, the collection of personal data of the users of the social network Facebook when they visit websites or apps – including those that may reveal information falling within one or more of the categories referred to in Article 9(1) of the GDPR – and, as the case may be, they enter information into them when they register or place online orders, then the linking of those data with those users’ social network accounts and, lastly, the use of those data.  
72      In that regard, it will be for the referring court to determine whether the data thus collected, on their own or by linking them with the Facebook accounts of the users concerned, actually allow such information to be revealed, irrespective of whether that information concerns a user of that network or any other natural person. However, given the referring court’s questions, it should be made clear that it appears, subject to verification by that court, that the processing of data relating to visits to the websites or apps in question may, in certain cases, reveal such information without it being necessary for those users to enter information into them when they register or place online orders.  
73      In the light of the foregoing, the answer to Question 2(a) is that Article 9(1) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories referred to in that provision relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user’s social network account and the use of those data by that operator, must be regarded as ‘processing of special categories of personal data’ within the meaning of that provision, which is in principle prohibited, subject to the derogations provided for in Article 9(2), where that data processing allows information falling within one of those categories to be revealed, irrespective of whether that information concerns a user of that network or any other natural person.  
   
Question 2(b)  
74      As regards Question 2(b), as reformulated in paragraph 65 above and which relates to the derogation laid down in Article 9(2)(e) of the GDPR, it must be recalled that, under that provision, the fundamental prohibition of any processing of special categories of personal data, established in Article 9(1) of the GDPR, does not apply in the circumstance where the processing relates to personal data which are ‘manifestly made public by the data subject’.  
75      As a preliminary point, it should be noted that, first, the derogation applies only to data which are manifestly made public ‘by the data subject’. Accordingly, it is not applicable to data concerning persons other than the person who made those data public.  
76      Second, in so far as it provides for an exception to the principle that the processing of special categories of personal data is prohibited, Article 9(2) of the GDPR must be interpreted strictly (see, to that effect, judgments of 17 September 2014,   
Baltic Agro  
, C-3/13, EU:C:2014:2227, paragraph 24 and the case-law cited, and of 6 June 2019,   
Weil  
, C-361/18, EU:C:2019:473, paragraph 43 and the case-law cited).  
77      It follows that, for the purposes of the application of the exception laid down in Article 9(2)(e) of the GDPR, it is important to ascertain whether the data subject had intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public.  
78      In that regard, as regards, first, visits to websites or apps to which one or more of the categories referred to in Article 9(1) of the GDPR relate, it should be noted that the user concerned does not in any way thereby intend to make public the fact that he or she has visited those sites or apps and the data from those visits which can be linked to his or her person. The latter can at most expect the operator of the site or app to have access to those data and to share them, as the case may be and subject to that user’s explicit consent, with certain third parties and not with the general public.  
79      Thus, it cannot be inferred from the mere visit to such websites or apps by a user that the personal data in question were manifestly made public by that user within the meaning of Article 9(2)(e) of the GDPR.  
80      Second, as regards the entering of information into those websites or apps and the clicking or tapping on buttons integrated into them, such as the ‘Like’ or ‘Share’ buttons or buttons enabling the user to identify himself or herself on a website or app using the login credentials linked to his or her Facebook user account, his or her telephone number or email address, it should be noted that these actions mean that the user interacts with the website or app in question, and, as the case may be, the website of the online social network, whereby the extent to which that interaction is public may vary in that it may be determined by the individual settings chosen by that user.  
81      In those circumstances, it is for the referring court to ascertain whether it is possible for the users concerned to decide, on the basis of settings selected with full knowledge of the facts, whether to make the information entered into the websites or apps in question and the data from clicking or tapping on buttons integrated into them accessible to the general public or, rather, to a more or less limited number of selected persons.  
82      When the users concerned actually have that choice, they can be regarded, when they voluntarily enter information into a website or app or when they click or tap on buttons integrated into them, as manifestly making public, within the meaning of Article 9(2)(e) of the GDPR, data relating to them only in the circumstance where, on the basis of individual settings selected with full knowledge of the facts, those users have clearly made the choice to have the data made accessible to an unlimited number of persons, which it is for the referring court to ascertain.  
83      By contrast, if no such individual settings are available, it must be held, in the light of what has been stated in paragraph 77 above, that, where users voluntarily enter information into a website or app or click or tap on buttons integrated into them, they must, in order to be deemed to have manifestly made those data public, have explicitly consented, on the basis of express information provided by that site or app prior to any such entering or clicking or tapping, to the data being viewed by any person having access to that site or app.  
84      In the light of the foregoing, the answer to Question 2(b) is that Article 9(2)(e) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories set out in Article 9(1) of the GDPR relate, the user does not manifestly make public, within the meaning of the first of those provisions, the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies.  
85      Where he or she enters information into such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the ‘Like’ or ‘Share’ buttons or buttons enabling the user to identify himself or herself on those sites or apps using login credentials linked to his or her social network user account, his or her telephone number or email address, that user manifestly makes public, within the meaning of Article 9(2)(e), the data thus entered or resulting from the clicking or tapping on those buttons only in the circumstance where he or she has explicitly made the choice beforehand, as the case may be on the basis of individual settings selected with full knowledge of the facts, to make the data relating to him or her publicly accessible to an unlimited number of persons.  
   
Q  
uestions  
 3 to 5  
86      By Questions 3 and 4, which it is appropriate to examine together, the referring court asks, in essence, whether and under what conditions points (b) and (f) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of such data, may be considered to be necessary for the performance of a contract to which the data subjects are party, within the meaning of point (b), or for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of point (f). That court asks, in particular, whether, to that end, certain interests which it explicitly lists constitute ‘legitimate interests’ within the meaning of the latter provision.  
87      By Question 5, the referring court asks, in essence, whether points (c) to (e) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that such processing of personal data can be regarded as necessary for compliance with a legal obligation to which the controller is subject, within the meaning of point (c), in order to protect the vital interests of the data subject or of another natural person, within the meaning of point (d), or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, within the meaning of point (e), where such processing is carried out, respectively, in order to respond to a legitimate request for certain data, to combat harmful behaviour and promote security, and to research for social good and promote safety, integrity and security.  
   
Preliminary observations  
88      As a preliminary point, it must be observed, first, that Questions 3 to 5 are raised on account of the fact that, according to the findings of the Federal Cartel Office in its decision of 6 February 2019, the users of the social network Facebook cannot be regarded as having given their consent to the processing of their data at issue in the main proceedings, within the meaning of point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR. It is therefore in that context that the referring court, while asking the Court by Question 6 in relation to that premiss, considers that it must ascertain whether that processing corresponds to one of the other conditions of lawfulness referred to in points (b) to (f) of the first subparagraph of Article 6(1)of that regulation.  
89      In that context, it should be noted that the operations entailing the collection, the linking and the use of the data, referred to in Questions 3 to 5, may include both sensitive data within the meaning of Article 9(1) of the GDPR and non-sensitive data. It must be made clear that, where a set of data containing both sensitive data and non-sensitive data is subject to such operations and is, in particular, collected   
en bloc  
 without it being possible to separate the data items from each other at the time of collection, the processing of that set of data must be regarded as being prohibited, within the meaning of Article 9(1) of the GDPR, if it contains at least one sensitive data item and none of the derogations in Article 9(2) of that regulation applies.  
90      Second, in order to answer Questions 3 to 5, it should be recalled that the first subparagraph of Article 6(1) of the GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being regarded as such, processing must fall within one of the cases provided for in that provision (judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 99 and the case-law cited).  
91      Under point (a) of the first subparagraph of Article 6(1) of that regulation, the processing of personal data is lawful if and to the extent that the data subject has given consent for one or more specific purposes.  
92      In the absence of such consent, or where that consent is not freely given, specific, informed and unambiguous, within the meaning of Article 4(11) of the GDPR, such processing is nevertheless justified where it meets one of the requirements of necessity mentioned in points (b) to (f) of the first subparagraph of Article 6(1) of that regulation.  
93      In that context, the justifications provided for in that latter provision, in so far as they allow the processing of personal data carried out in the absence of the data subject’s consent to be made lawful, must be interpreted restrictively (see, to that effect, judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 73 and the case-law cited).  
94      Furthermore, as the Court has held, where it can be found that the processing of personal data is necessary in respect of one of the justifications provided for in points (b) to (f) of the first subparagraph of Article 6(1) of the GDPR, it is not necessary to determine whether that processing also falls within the scope of another of those justifications (see, to that effect, judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 71).  
95      It should finally be noted that, in accordance with Article 5 of the GDPR, the controller bears the burden of proving that those data are collected, inter alia, for specified, explicit and legitimate purposes and that they are processed lawfully, fairly and in a transparent manner in relation to the data subject. In addition, according to Article 13(1)(c) of that regulation, where personal data are collected from the data subject, the controller must inform the data subject of the purposes of the processing for which those data are intended as well as the legal basis for the processing.  
96      Although it is for the referring court to determine whether the various elements of the processing at issue in the main proceedings are justified by one or other of the necessity requirements referred to in points (b) to (f) of the first subparagraph of Article 6(1) of the GDPR, the Court can nevertheless provide it with useful guidance to enable it to resolve the dispute before it.  
   
Questions 3 and 4  
97      As regards, in the first place, point (b) of the first subparagraph of Article 6(1) of the GDPR, that provision provides that processing of personal data is lawful if it is ‘necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract’.  
98      In that regard, in order for the processing of personal data to be regarded as necessary for the performance of a contract, within the meaning of that provision, it must be objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject. The controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur.  
99      The fact that such processing may be referred to in the contract or may be merely useful for the performance of the contract is, in itself, irrelevant in that regard. The decisive factor for the purposes of applying the justification set out in point (b) of the first subparagraph of Article 6(1) of the GDPR is rather that the processing of personal data by the controller must be essential for the proper performance of the contract concluded between the controller and the data subject and, therefore, that there are no workable, less intrusive alternatives.  
100    In that regard, as the Advocate General observed in point 54 of his Opinion, where the contract consists of several separate services or elements of a service that can be performed independently of one another, the applicability of point (b) of the first subparagraph of Article 6(1) of the GDPR should be assessed in the context of each of those services separately.  
101    In the present case, in the context of the justifications that are capable of falling within the scope of that provision, the referring court mentions, as elements intended to ensure the proper performance of the contract concluded between Meta Platforms Ireland and its users, personalised content and the consistent and seamless use of the Meta group’s own services.  
102    As regards, first, the justification based on personalised content, it is important to note that, although such a personalisation is useful to the user, in so far as it enables the user, inter alia, to view content corresponding to a large extent to his or her interests, the fact remains that, subject to verification by the referring court, personalised content does not appear to be necessary in order to offer that user the services of the online social network. Those services may, where appropriate, be provided to the user in the form of an equivalent alternative which does not involve such a personalisation, such that the latter is not objectively indispensable for a purpose that is integral to those services.  
103    As regards, second, the justification based on the consistent and seamless use of the Meta group’s own services, it is apparent from the file before the Court that there is no obligation to subscribe to the various services offered by the Meta group in order to create a user account in the social network Facebook. The various products and services offered by that group can be used independently of each other and the use of each product or service is based on the conclusion of a separate user agreement.  
104    Therefore, and subject to verification by the referring court, the processing of personal data from services offered by the Meta group, other than the online social network service, does not appear to be necessary for the latter service to be provided.  
105    As regards, in the second place, point (f) of the first subparagraph of Article 6(1) of the GDPR, that provision provides that the processing of personal data is lawful only if it is ‘necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child’.  
106    As the Court has already held, that provision lays down three cumulative conditions so that the processing of personal data covered by that provision is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or fundamental freedoms and rights of the person concerned by the data protection do not take precedence over the legitimate interest of the controller or of a third party (judgment of 17 June 2021,   
M.I.C.M.  
, C-597/19, EU:C:2021:492, paragraph 106 and the case-law cited).  
107    First, with regard to the condition relating to the pursuit of a legitimate interest, it must be stated that, according to Article 13(1)(d) of the GDPR, it is the responsibility of the controller, at the time when personal data relating to a data subject are collected from that person, to inform him or her of the legitimate interests pursued where that processing is based on point (f) of the first subparagraph of Article 6(1) of that regulation.  
108    Second, with regard to the condition that the processing of personal data be necessary for the purposes of the legitimate interests pursued, that condition requires the referring court to ascertain that the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 22 June 2021,   
Latvijas Republikas Saeima (Penalty points)  
, C-439/19, EU:C:2021:504, paragraph 110 and the case-law cited).  
109    In this context, it should also be recalled that the condition relating to the need for processing must be examined in conjunction with the ‘data minimisation’ principle enshrined in Article 5(1)(c) of the GDPR, in accordance with which personal data must be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’ (see, to that effect, judgment of 11 December 2019,   
Asociaţia de Proprietari bloc M5A-ScaraA  
, C-708/18, EU:C:2019:1064, paragraph 48).  
110    Third, with regard to the condition that the interests or fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interests of the controller or of a third party, the Court has already held that that condition entails a balancing of the opposing rights and interests at issue which depends in principle on the specific circumstances of the particular case and that, consequently, it is for the referring court to carry out that balancing exercise, taking account of those specific circumstances (judgment of 17 June 2021,   
M.I.C.M.  
, C-597/19, EU:C:2021:492, paragraph 111 and the case-law cited).  
111    In this respect, it is apparent from the very wording of point (f) of the first subparagraph of Article 6(1) of the GDPR that it is necessary, in such a balancing exercise, to pay particular attention to the situation where the data subject is a child. According to recital 38 of that regulation, children merit specific protection with regard to the processing of their personal data because they may be less aware of the risks, consequences and safeguards concerned and of their rights related to such processing of personal data. Thus, such specific protection should, in particular, apply to the processing of personal data of children for the purposes of marketing or creating personality or user profiles or offering services aimed directly at children.  
112    Furthermore, as can be seen from recital 47 of the GDPR, the interests and fundamental rights of the data subject may in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing.  
113    In the present case, in the context of the justifications that are capable of falling within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR, the referring court mentions personalised advertising, network security, product improvement, the sharing of informing with law-enforcement agencies, the fact that the user is a minor, research and innovation for social good and the offer of services for commercial communication intended for the user and of analytics tools intended for advertisers and other business partners, enabling them to evaluate their performance.  
114    In that regard, it should be noted at the outset that the request for a preliminary ruling does not contain any explanation as to how research and innovation for social good or the fact that the user is a minor could justify, as legitimate interests within the meaning of point (f) of the first subparagraph of Article 6(1) of the GDPR, the collection and use of the data in question. Consequently, the Court is not in a position to rule on this matter.  
115    First, with regard to personalised advertising, it must be borne in mind that, according to recital 47 of the GDPR, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest of the controller.  
116    However, such processing must also be necessary in order to achieve that interest and the interests or fundamental freedoms and rights of the data subject must not override that interest. In the context of that balancing of the opposing rights at issue, namely, those of the controller, on the one hand, and those of the data subject, on the other, account must be taken, as has been noted in paragraph 112 above, in particular of the reasonable expectations of the data subject as well as the scale of the processing at issue and its impact on that person.  
117    In this regard, it is important to note that, despite the fact that the services of an online social network such as Facebook are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user’s personal data, without his or her consent, for the purposes of personalised advertising. In those circumstances, it must be held that the interests and fundamental rights of such a user override the interest of that operator in such personalised advertising by which it finances its activity, with the result that the processing by that operator for such purposes cannot fall within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR.  
118    Furthermore, the processing at issue in the main proceedings is particularly extensive since it relates to potentially unlimited data and has a significant impact on the user, a large part – if not almost all – of whose online activities are monitored by Meta Platforms Ireland, which may give rise to the feeling that his or her private life is being continuously monitored.  
119    Second, as regards the objective of ensuring network security, that objective, as stated in recital 49 of the GDPR, constitutes a legitimate interest of Meta Platforms Ireland, capable of justifying the processing operation at issue in the main proceedings.  
120    However, as regards the need for that processing for the purposes of that legitimate interest, the referring court will have to ascertain whether and to what extent the processing of personal data collected from sources outside the social network Facebook is actually necessary to ensure that the internal security of that network is not compromised.  
121    In that context, as noted in paragraphs 108 and 109 above, it will also have to ascertain whether the legitimate data processing interest pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental freedoms and rights of the data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter and whether the ‘data minimisation’ principle enshrined in Article 5(1)(c) of the GDPR has been observed.  
122    Third, as regards the ‘product improvement’ objective, it cannot be ruled out from the outset that the controller’s interest in improving the product or service with a view to making it more efficient and thus more attractive can constitute a legitimate interest capable of justifying the processing of personal data and that such processing may be necessary in order to pursue that interest.  
123    However, subject to final assessment by the referring court in that respect, it appears doubtful whether, as regards the data processing at issue in the main proceedings, the ‘product improvement’ objective, given the scale of that processing and its significant impact on the user, as well as the fact that the user cannot reasonably expect those data to be processed by Meta Platforms Ireland, may override the interests and fundamental rights of such a user, particularly in the case where that user is a child.  
124    Fourth, as regards the objective referred to by the referring court, relating to the sharing of information with law-enforcement agencies in order to prevent, detect and prosecute criminal offences, it must be held that that objective is not capable, in principle, of constituting a legitimate interest pursued by the controller, within the meaning of point (f) of the first subparagraph of Article 6(1) of the GDPR. A private operator such as Meta Platforms Ireland cannot rely on such a legitimate interest, which is unrelated to its economic and commercial activity. Conversely, that objective may justify processing by such an operator where it is objectively necessary for compliance with a legal obligation to which that operator is subject.  
125    In the light of all the foregoing, the answer to Questions 3 and 4 is that point (b) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the performance of a contract to which the data subjects are party, within the meaning of that provision, only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur.  
126    Point (f) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that such processing can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of that provision, only on condition that the operator has informed the users from whom the data have been collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party.  
   
Question 5  
127    In the first place, in so far as that question refers to points (c) and (e) of the first subparagraph of Article 6(1) of the GDPR, it must be recalled that, under point (c), processing of personal data is lawful if it is necessary for compliance with a legal obligation to which the controller is subject. In addition, under point (e), processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller is also lawful.  
128    Article 6(3) of the GDPR specifies, inter alia, in respect of those two situations in which processing is lawful, that the processing must be based on EU law or on Member State law to which the controller is subject, and that that legal basis must meet an objective of public interest and be proportionate to the legitimate aim pursued.  
129    In the present case, the referring court seeks to ascertain whether the processing of personal data, such as that at issue in the main proceedings, may be regarded as justified in the light of point (c) of the first subparagraph of Article 6(1) of the GDPR, where it seeks to ‘respond to a legitimate request for certain data’, and, in the light of point (e) of the first subparagraph of Article 6(1) of that regulation, where its purpose is to ‘research for social good’ and it seeks to ‘promote safety, integrity and security’.  
130    However, it should be noted that the referring court has not provided the Court of Justice with any material enabling it to give a specific ruling in this respect.  
131    It will therefore be for that court to ascertain, in the light of the conditions set out in paragraph 128 above, whether that processing can be regarded as being justified by the stated purposes.  
132    In particular, given the observations made in paragraph 124 above, it will be for the referring court, inter alia, to inquire, for the purposes of applying point (c) of the first subparagraph of Article 6(1) of the GDPR, whether Meta Platforms Ireland is under a legal obligation to collect and store personal data in a preventive manner in order to be able to respond to any request from a national authority seeking to obtain certain data relating to its users.  
133    Similarly, it will be for that court to assess, in the light of point (e) of the first subparagraph of Article 6(1) of the GDPR, whether Meta Platforms Ireland was entrusted with a task carried out in the public interest or in the exercise of official authority, in particular with a view of carrying out research for the social good and to promote safety, integrity and security, bearing in mind that, given the type of activity and the essentially economic and commercial nature thereof, it seems unlikely that that private operator was entrusted with such a task.  
134    In addition, the referring court will, if necessary, have to determine whether, in view of the scale of the data processing by Meta Platforms Ireland and of its significant incidence on the users of the social network Facebook, that processing is carried out only in so far as is strictly necessary.  
135    As regards, in the second place, point (d) of the first subparagraph of Article 6(1) of the GDPR, that provision provides that the processing of personal data is lawful where it is necessary in order to protect the vital interests of the data subject or of another natural person.  
136    As can be seen from recital 46 of that regulation, that provision covers the specific situation in which the processing of personal data is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. In that regard, the recital cites by way of example, inter alia, humanitarian purposes, such as monitoring epidemics and their spread, as well as situations of humanitarian emergencies, such as situations of natural and man-made disasters.  
137    It follows from those examples and from the strict interpretation to be given to point (d) of the first subparagraph of Article 6(1) of the GDPR that, in view of the nature of the services provided by the operator of an online social network, such an operator, whose activity is essentially economic and commercial in nature, cannot rely on the protection of an interest which is essential for the life of its users or of another person in order to justify, absolutely and in a purely abstract and preventive manner, the lawfulness of data processing such as that at issue in the main proceedings.  
138    In the light of the foregoing, the answer to Question 5 is that point (c) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, is justified, under that provision, where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, where that legal basis meets an objective of public interest and is proportionate to the legitimate aim pursued and where that processing is carried out only in so far as is strictly necessary.  
139    Points (d) and (e) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that such processing of personal data cannot, in principle and subject to verification by the referring court, be regarded as necessary in order to protect the vital interests of the data subject or of another natural person, within the meaning of point (d), or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, within the meaning of point (e).  
   
Q  
uestion  
 6  
140    By Question 6, the referring court asks, in essence, whether point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR must be interpreted as meaning that consent given by the user of an online social network to the operator of such a network may be regarded as satisfying the conditions of validity laid down in Article 4(11) of that regulation, in particular the condition that that consent must be freely given, where that operator holds a dominant position on the market for online social networks.  
141    Point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR require the data subject’s consent for the purposes of, respectively, processing his or her personal data for one or more specific purposes and processing special categories of data referred to in Article 9(1).  
142    Article 4(11) of the GDPR, for its part, defines ‘consent’ as meaning ‘any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.  
143    In the light of the referring court’s questions, it is important to recall, in the first place, that, according to recital 42 of the GDPR, consent cannot be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.  
144    In the second place, recital 43 of that regulation states that, in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data where there is a clear imbalance between the data subject and the controller. That recital also clarifies that consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.  
145    In the third place, Article 7(4) of the GDPR provides that when assessing whether consent is freely given, utmost account must be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.  
146    It is on the basis of those considerations that Question 6 must be answered.  
147    In that regard, it should be noted that, admittedly, the fact that the operator of an online social network, as controller, holds a dominant position on the social network market does not, as such, prevent the users of that social network from validly giving their consent, within the meaning of Article 4(11) of the GDPR, to the processing of their personal data by that operator.  
148    The fact remains that, as the Advocate General observed, in essence, in point 75 of his Opinion, such a circumstance must be taken into consideration in assessing whether the user of that network has validly and, in particular, freely given consent, since that circumstance is liable to affect the freedom of choice of that user, who might be unable to refuse or withdraw consent without detriment, as stated in recital 42 of the GDPR.  
149    Furthermore, the existence of such a dominant position may create a clear imbalance, within the meaning of recital 43 of the GDPR, between the data subject and the controller, that imbalance favouring, inter alia, the imposition of conditions that are not strictly necessary for the performance of the contract, which must be taken into account under Article 7(4) of that regulation. In that context, it must be borne in mind that, as stated in paragraphs 102 to 104 above, it does not appear, subject to verification by the referring court, that the processing at issue in the main proceedings is strictly necessary for the performance of the contract between Meta Platforms Ireland and the users of the social network Facebook.  
150    Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.  
151    Moreover, given the scale of the processing of the data in question and the significant impact of that processing on the users of that network as well as the fact that those users cannot reasonably expect data other than those relating to their conduct within the social network to be processed by the operator of that network, it is appropriate, within the meaning of recital 43, to have the possibility of giving separate consent for the processing of the latter data, on the one hand, and the off-Facebook data, on the other. It is for the referring court to ascertain whether such a possibility exists, in the absence of which the consent of those users to the processing of the off-Facebook data must be presumed not to be freely given.  
152    Finally, it must be borne in mind that, pursuant to Article 7(1) of the GDPR, where processing is based on consent, it is the controller who bears the burden of demonstrating that the data subject has consented to the processing of his or her personal data.  
153    It is in the light of those criteria and of a detailed examination of all the circumstances of the case that the referring court will have to determine whether the users of the social network Facebook have validly and, in particular, freely given their consent to the processing at issue in the main proceedings.  
154    In the light of the foregoing, the answer to Question 6 is that point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR must be interpreted as meaning that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of that regulation, to the processing of their personal data by that operator. This is nevertheless an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove.  
   
Costs  
155    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 51 et seq. of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as well as Article 4(3) TEU  
must be interpreted as meaning that, subject to compliance with its duty of sincere cooperation with the supervisory authorities, a competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position by an undertaking within the meaning of Article 102 TFEU, that that undertaking’s general terms of use relating to the processing of personal data and the implementation thereof are not consistent with that regulation, where that finding is necessary to establish the existence of such an abuse.  
In view of this duty of sincere cooperation, the national competition authority cannot depart from a decision by the competent national supervisory authority or the competent lead supervisory authority concerning those general terms or similar general terms. Where it has doubts as to the scope of such a decision, where those terms or similar terms are, simultaneously, under examination by those authorities, or where, in the absence of an investigation or decision by those authorities, the competition authority takes the view that the terms in question are not consistent with Regulation 2016/679, it must consult and seek the cooperation of those supervisory authorities in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment. In the absence of any objection on their part or of any reply within a reasonable time, the national competition authority may continue its own investigation;  
2.        
Article 9(1) of Regulation 2016/679  
must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories referred to in that provision relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user’s social network account and the use of those data by that operator, must be regarded as ‘processing of special categories of personal data’ within the meaning of that provision, which is in principle prohibited, subject to the derogations provided for in Article 9(2), where that data processing allows information falling within one of those categories to be revealed, irrespective of whether that information concerns a user of that network or any other natural person;  
3.        
Article 9(2)(e) of Regulation 2016/679  
must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories set out in Article 9(1) of that regulation relate, the user does not manifestly make public, within the meaning of the first of those provisions, the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies;  
Where he or she enters information into such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the ‘Like’ or ‘Share’ buttons or buttons enabling the user to identify himself or herself on those sites or apps using login credentials linked to his or her social network user account, his or her telephone number or email address, that user manifestly makes public, within the meaning of Article 9(2)(e), the data thus entered or resulting from the clicking or tapping on those buttons only in the circumstance where he or she has explicitly made the choice beforehand, as the case may be on the basis of individual settings selected with full knowledge of the facts, to make the data relating to him or her publicly accessible to an unlimited number of persons;  
4.        
Point (b) of the first subparagraph of Article 6(1) of Regulation 2016/679  
must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the performance of a contract to which the data subjects are party, within the meaning of that provision, only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur;  
5.        
Point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679  
must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of that provision, only on condition that the operator has informed the users from whom the data have been collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party;  
6.        
Point (c) of the first subparagraph of Article 6(1) of Regulation 2016/679  
must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, is justified, under that provision, where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, where that legal basis meets an objective of public interest and is proportionate to the legitimate aim pursued and where that processing is carried out only in so far as is strictly necessary;  
7.        
Points (d) and (e) of the first subparagraph of Article 6(1) of Regulation 2016/679  
must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, cannot, in principle and subject to verification by the referring court, be regarded as necessary in order to protect the vital interests of the data subject or of another natural person, within the meaning of point (d), or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, within the meaning of point (e);  
8.        
Point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of Regulation 2016/679  
must be interpreted as meaning that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of that regulation, to the processing of their personal data by that operator. This is nevertheless an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove.

ID: b0add817-e00d-4de2-94b3-38d3c5fa9c57

of 12 Jan 2023, C-132/21 (  
Nemzeti Adatvédelmi és Információszabadság Hatóság  
)  
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Right to lodge a complaint with a supervisory authority   
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Right to an effective remedy against a supervisory authority   
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Right to an effective judicial remedy against a controller or processor   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
   
JUDGMENT OF THE COURT (First Chamber)  
12 January 2023 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Articles 77 to 79 – Remedies – Parallel exercise – Relationship – Procedural autonomy – Effectiveness of the protection rules established by that regulation – Consistent and homogeneous application of those rules throughout the European Union – Article 47 of the Charter of Fundamental Rights of the European Union)  
In Case C-132/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Fővárosi Törvényszék (Budapest High Court, Hungary), made by decision of 2 March 2021, received at the Court on 3 March 2021, in the proceedings  
BE  
v  
Nemzeti Adatvédelmi és Információszabadság Hatóság,  
interested party:  
Budapesti Elektromos Művek Zrt.,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, L. Bay Larsen, Vice-President, acting as Judge of the First Chamber, P.G. Xuereb, A. Kumin and I. Ziemele (Rapporteur), Judges,  
Advocate General: J. Richard de la Tour,  
Registrar: I. Illéssy, Administrator,  
having regard to the written procedure and further to the hearing on 11 May 2022,  
after considering the observations submitted on behalf of:  
–        BE, by I. Kulcsár, ügyvéd,  
–        the Nemzeti Adatvédelmi és Információszabadság Hatóság, by G. Barabás, jogtanácsos, G.J. Dudás and Á. Hargita, ügyvédek,  
–        the Hungarian Government, by Zs. Biró-Tóth and M.Z. Fehér, acting as Agents,  
–        the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by E. De Bonis and M.F. Severi, avvocati dello Stato,  
–        the Polish Government, by B. Majczyna and J. Sawicka, acting as Agents,  
–        the European Commission, by H. Kranenborg, Zs. Teleki and P.J.O. Van Nuffel, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 8 September 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 77(1), Article 78(1) and Article 79(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).  
2        The request has been made in proceedings between BE and the Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information, Hungary; ‘the supervisory authority’) concerning the refusal of BE’s request to be sent extracts from the sound recording of the general meeting of a company’s shareholders in which he had taken part.  
   
Legal context  
   
European Union law  
3        Under recitals 10, 11, 141 and 143 of Regulation 2016/679:  
‘(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …   
(11)      Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data …   
…  
(141)      Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter [of Fundamental Rights of the European Union] if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. …   
…  
(143)      … each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. … Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State’s procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.’  
4        Articles 60 to 63 of that regulation establish cooperation, mutual assistance and consistency mechanisms between the supervisory authorities of the Member States.  
5        Article 77(1) of that regulation provides:  
‘Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.’  
6        Article 78(1) of that regulation states:  
‘Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.’  
7        Article 79(1) of Regulation 2016/679 provides:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’  
8        Article 81 of that regulation, entitled ‘Suspension of proceedings’, is worded as follows:  
‘1.      Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.  
2.      Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seised may suspend its proceedings.  
3.      Where those proceedings are pending at first instance, any court other than the court first seised may also, on the application of one of the parties, decline jurisdiction if the court first seised has jurisdiction over the actions in question and its law permits the consolidation thereof.’  
   
Hungarian law  
9        Paragraph 22 of the az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Law [No] CXII of 2011 on the right to self-determination as regards information and freedom of information), in the version applicable to the dispute in the main proceedings, provides:  
‘In the exercise of his or her rights, the data subject may, in accordance with the provisions of Chapter VI:  
(a)      ask [the supervisory authority] to launch an investigation into the lawfulness of a measure adopted by the controller, in the case where the controller has limited the exercise of the rights enjoyed by the data subject under Paragraph 14 or has refused a request by which the data subject has sought to exercise his or her rights, and   
(b)      ask [the supervisory authority] to conduct an administrative data protection procedure, in the case where the data subject considers that, in processing his or her personal data, the controller or the processor acting either on the controller’s behalf or on the basis of the controller’s instructions has failed to meet requirements regarding the processing of personal data which are laid down in legislation or in a binding legal act of the European Union.’  
10      Paragraph 23 of Law [No] CXII of 2011, in the version applicable to the dispute in the main proceedings, states:  
‘1.      The data subject may bring legal proceedings against the controller, or against the processor in connection with processing operations coming within the processor’s sphere of activity, in the case where the data subject considers that, in processing his or her personal data, the controller or the processor acting either on the controller’s behalf or on the basis of the controller’s instructions, has done so in disregard of requirements regarding the processing of personal data which are laid down in legislation or in a binding legal act of the European Union.  
…  
4.      Judicial proceedings shall also be open to participation to persons who otherwise lack  
 locus standi  
. [The supervisory authority] may intervene in those proceedings in support of the claims of the data subject.  
5.      If the court upholds the action, it shall find that an infringement has been committed and order the controller or the processor to:  
(a)      cease the unlawful data processing operation;  
(b)      restore the lawfulness of data processing; and/or  
(c)      adopt precisely defined conduct in order to ensure that the data subject can exercise his or her rights,  
and, if necessary, at the same time give a ruling on any claims for damages for material and non-material harm.’  
   
The facts of the dispute in the main proceedings and the questions referred for a preliminary ruling  
11      On 26 April 2019, BE attended the general meeting of a public limited company of which he is a shareholder and, at that time, put questions to the members of the board of directors of that company and to other persons attending that general meeting. Subsequently, BE asked that company, as the personal data controller, to send him the sound recording made at the general meeting.  
12      The company in question made available to BE only the excerpts from that recording which reproduced his contributions, excluding those of the other persons attending the general meeting in question.  
13      BE then asked the supervisory authority (i) to declare that, by failing to provide him with the recording including the answers given to his questions, the company had acted unlawfully and in breach of Regulation 2016/679 and (ii) to order that company to send him the recording in question. The supervisory authority refused that request by decision of 29 November 2019.  
14      BE brought proceedings before the referring court against that decision of the supervisory authority on the basis of Article 78(1) of that regulation, seeking, principally, that the decision be varied, and, in the alternative, that it be annulled.  
15      At the same time as approaching the supervisory authority, BE initiated another set of proceedings, this time on the basis of Article 79(1) of that regulation, before a civil court, namely the Fővárosi Ítélőtábla (Budapest Regional Court of Appeal, Hungary), against the decision of the controller.  
16      Although one set of proceedings are still pending before the referring court, the Fővárosi Ítélőtábla (Budapest Regional Court of Appeal, Hungary) upheld the action in the other set of proceedings, by a judgment which has become final, on the ground that the controller had infringed BE’s right of access to his personal data.  
17      The referring court states that it has to examine the same facts and the same allegation of infringement of Regulation 2016/679 as those on which the Fővárosi Ítélőtábla (Budapest Regional Court of Appeal, Hungary) has already given a final ruling. It questions how it should view the relationship between, on the one hand, a civil court’s assessment of the lawfulness of a decision adopted by the personal data controller and, on the other, the administrative procedure which led to the adoption of the supervisory authority’s decision, referred to in paragraph 13 of the present judgment, which forms the subject matter of the action pending before the referring court and, in particular, whether one remedy might take priority over the other.  
18      According to that court, the parallel exercise of the remedies provided for in Articles 77 to 79 of Regulation 2016/679 could give rise to contradictory decisions concerning identical facts.  
19      In its view, such a situation would risk undermining legal certainty as regards both private persons and supervisory authorities.  
20      The referring court states that, having regard to the independence of the supervisory authorities and to the fact that their powers, as defined by Regulation 2016/679, are dominant in the personal data protection system, the tasks and powers of those authorities would be undermined if they were bound, in their assessments, by those of a civil court that was seised at an earlier stage of the same facts on the basis of Article 79(1) of that regulation.  
21      Since the provisions of that regulation do not lay down any rule of priority in respect of the remedies provided for in Articles 77 to 79 thereof, the referring court considers that it is for the Court of Justice to provide clarification on the relationship between those remedies.  
22      In those circumstances, the Fővárosi Törvényszék (Budapest High Court, Hungary) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must Articles 77(1) and 79(1) of [Regulation 2016/679] be interpreted as meaning that the administrative appeal provided for in Article 77 [of that regulation] constitutes an instrument for the exercise of public rights, whereas the legal action provided for in Article 79 [thereof] constitutes an instrument for the exercise of private rights? If so, does this support the inference that the supervisory authority, which is responsible for hearing and determining administrative appeals, has priority competence to determine the existence of an infringement?  
(2)      In the event that the data subject – in whose opinion the processing of personal data relating to him has infringed Regulation 2016/679 – simultaneously exercises his right to lodge a complaint under Article 77(1) of that regulation and his right to bring a legal action under Article 79(1) of the same regulation, may an interpretation in accordance with Article 47 of the Charter of Fundamental Rights be regarded as meaning:  
(a)      that the supervisory authority and the court have an obligation to examine the existence of an infringement independently and may therefore even arrive at different outcomes; or  
(b)      that the supervisory authority’s decision takes priority when it comes to the assessment as to whether an infringement has been committed, regard being had to the powers provided for in Article 51(1) of Regulation 2016/679 and those conferred by Article 58(2)(b) and (d) of that regulation?  
(3)      Must the independence of the supervisory authority, ensured by Articles 51(1) and 52(1) of Regulation 2016/679, be interpreted as meaning that that authority, when conducting and adjudicating upon complaint proceedings under Article 77 [of that regulation], is independent of whatever ruling may be given by final judgment by the court having jurisdiction under Article 79 [thereof], with the result that it may even adopt a different decision in respect of the same alleged infringement?’  
   
Consideration of the questions referred  
   
Admissibility  
23      The European Commission has doubts as to the admissibility of the questions referred. It submits that, as is apparent from the request for a preliminary ruling, on the date of that request, both the supervisory authority and the civil court had given their decisions, with the result that those questions are, as such, hypothetical. According to the Commission, in reality, the referring court is uncertain as to the relationship between the respective decisions of two national courts, namely the administrative court and the civil court. However, that question was not formulated in the order for reference.  
24      In that regard, it should be observed that questions on the interpretation of EU law referred by a national court in the factual and legislative context which that court is responsible for defining, the accuracy of which is not a matter for the Court to determine, enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its object, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 10 February 2022,   
Bezirkshauptmannschaft Hartberg-Fürstenfeld (Limitation period)  
, C-219/20, EU:C:2022:89, paragraph 20 and the case-law cited).  
25      In addition, the request for a preliminary ruling must contain, in accordance with Article 94(c) of the Rules of Procedure of the Court of Justice, a statement of the reasons which prompted the referring court or tribunal to inquire about the interpretation of certain provisions of EU law, and the relationship between those provisions and the national legislation applicable to the main proceedings.  
26      In the present case, it is, admittedly, not disputed that the supervisory authority, which had been seised on the basis of Article 77(1) of Regulation 2016/679, gave its decision before the civil court which ruled on the action brought by BE on the basis of Article 79(1) of that regulation had been seised. It is apparent from the facts set out by the referring court that that action gave rise to a judgment which has become final. In addition, it is true that the referring court has mentioned only those two provisions in the questions which it has referred to the Court for a preliminary ruling.  
27      However, the fact that a question submitted by the referring court refers only to certain provisions of EU law does not mean that the Court may not provide the national court with all the guidance on points of interpretation that may be of assistance in adjudicating on the case pending before it, whether or not that court has referred to those points in its questions. It is, in this regard, for the Court to extract from all the information provided by the referring court, in particular from the grounds of the decision to make the reference, the points of EU law which require interpretation in view of the subject matter of the dispute (judgment of 10 February 2022,   
Bezirkshauptmannschaft Hartberg-Fürstenfeld (Limitation period)  
, C-219/20, EU:C:2022:89, paragraph 34 and the case-law cited).  
28      First, the referring court states that, pursuant to national procedural law, it is not bound by the final judgment delivered by the civil court which ruled on the action brought by BE on the basis of Article 79(1) of Regulation 2016/679. Second, since BE has not withdrawn his action before the referring court, brought on the basis of Article 78(1) of that regulation, seeking the variation or annulment of the decision of the supervisory authority referred to in paragraph 13 of the present judgment, it is for the referring court to rule on the lawfulness of that decision, which was given before the civil court’s judgment had been delivered.  
29      Thus, by its questions, the referring court, which is seised of an action, on the basis of Article 78(1) of Regulation 2016/679, against the supervisory authority’s decision given on the basis of Article 77(1) thereof, seeks to ascertain whether, under the provisions of that regulation, the final judgment delivered by a court seised on the basis of Article 79(1) thereof is binding as regards the finding that there has – or has not – been an infringement of the rights guaranteed by that same regulation.  
30      In those circumstances, in order to provide a useful answer to the referring court, it should be considered that, by its questions, which it is appropriate to examine together, that court asks, in essence, whether Article 77(1), Article 78(1) and Article 79(1) of Regulation 2016/679, read in the light of Article 47 of the Charter of Fundamental Rights (‘the Charter’), are to be interpreted as meaning that the remedies provided for in Article 77(1) and Article 78(1) of that regulation, on the one hand, and Article 79(1) thereof, on the other, are capable of being exercised concurrently with and independently of each other, or whether one of them has priority over the other.  
31      The questions referred, as thus reformulated, are therefore admissible.  
   
Substance  
32      As a preliminary point, it should be borne in mind that, in accordance with the Court’s settled case-law, in interpreting a provision of EU law it is necessary to consider not only its wording but also its context and the objectives pursued by the legislation of which it forms part (judgment of 2 December 2021,   
Vodafone Kabel Deutschland  
, C-484/20, EU:C:2021:975, paragraph 19 and the case-law cited).  
33      As regards the wording of the provisions of Regulation 2016/679 referred to in paragraph 30 of the present judgment, it must be borne in mind, first of all, that Article 77(1) of that regulation states that it is ‘without prejudice to any other administrative or judicial remedy’ that every data subject is to have the right to lodge a complaint with a supervisory authority. Next, under Article 78(1) of that regulation, each natural or legal person is to have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them ‘without prejudice to any other administrative or non-judicial remedy’. Lastly, Article 79(1) of that regulation guarantees each data subject the right to an effective judicial remedy ‘without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77’.  
34      Thus, those provisions of Regulation 2016/679 offer different remedies to persons claiming that that regulation has been infringed, it being understood that each of those remedies must be capable of being exercised ‘without prejudice’ to the others.  
35      It follows, first of all, from the wording of those provisions that Regulation 2016/679 does not provide for any priority or exclusive competence or jurisdiction or for any rule of precedence in respect of the assessment carried out by the authority or by the courts referred to therein as to whether there is an infringement of the rights conferred by that regulation. The remedy provided for in Article 78(1) of that regulation, the purpose of which is to examine the lawfulness of the decision of a supervisory authority adopted on the basis of Article 77 thereof, and the remedy provided for in Article 79(1) of that regulation may therefore be exercised concurrently with and independently of each other.  
36      Next, that finding is borne out by the context of the provisions of Regulation 2016/679 at issue.  
37      Although the EU legislature has expressly regulated the relationship between the remedies provided for by Regulation 2016/679 in the event of the supervisory authorities or courts of several Member States being seised simultaneously in respect of an instance of processing of personal data carried out by the same controller, it must be observed that this is not the case as regards the remedies provided for in Articles 77 to 79 of that regulation.  
38      Articles 60 to 63 of Regulation 2016/679 provide for cooperation, mutual assistance and coordination mechanisms under which the supervisory authorities are to provide each other with mutual assistance, inform each other and conduct joint operations with a view to ensuring a consistent and effective application of the provisions of that regulation throughout the European Union.  
39      In addition, Article 81(2) and (3) of that regulation lays down rules concerning cases where several courts of different Member States have been seised.  
40      By contrast, Regulation 2016/679 does not lay down such rules in respect of cases where a complaint has been made to a supervisory authority and judicial proceedings have been brought within the same Member State concerning the same instance of processing of personal data.  
41      Furthermore, it follows from Article 78(1) of Regulation 2016/679, read in the light of recital 143 of that regulation, that courts seised of an action against a decision of a supervisory authority should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.  
42      Lastly, regarding the objectives pursued by that regulation, it is apparent, in particular, from recital 10 thereof that the aim of that regulation is to ensure a high level of protection of natural persons with regard to the processing of personal data within the European Union. Recital 11 of that regulation states, moreover, that effective protection of such data requires the strengthening of the rights of data subjects. As the Advocate General observed in point 55 of his Opinion, the EU legislature’s decision to leave to data subjects the option to exercise the remedies provided for in Article 77(1) and Article 78(1) of Regulation 2016/679, on the one hand, and Article 79(1) thereof, on the other, concurrently with and independently of each other is consistent with the objective of that regulation.  
43      Regulation 2016/679 requires, inter alia, the competent authorities of the Member States to ensure a high level of protection of the rights guaranteed in Article 16 TFEU and Article 8 of the Charter (see, to that effect, judgment of 15 June 2021,   
Facebook Ireland and Others  
, C-645/19, EU:C:2021:483, paragraph 45).  
44      Making several remedies available also strengthens the objective set out in recital 141 of Regulation 2016/679 of guaranteeing for every data subject who considers that his or her rights under that regulation are infringed the right to an effective judicial remedy in accordance with Article 47 of the Charter.  
45      In the absence of EU rules governing the matter, it is for each Member State, in accordance with the principle of the procedural autonomy of the Member States, to lay down the detailed rules of administrative and judicial procedures intended to ensure a high level of protection of rights which individuals derive from EU law.  
46      Accordingly, it is for the referring court to determine, on the basis of the national procedural provisions, how the remedies provided for by Regulation 2016/679 must be implemented in a situation such as that at issue in the main proceedings.  
47      That said, the detailed rules for the implementation of those concurrent and independent remedies should not call into question the effectiveness and effective protection of the rights guaranteed by that regulation.  
48      Those detailed rules must not be less favourable than those governing similar domestic actions (principle of equivalence); nor must they render practically impossible or excessively difficult the exercise of rights conferred by EU law (principle of effectiveness) (see, to that effect, judgment of 14 July 2022,   
EPIC Financial Consulting  
, C-274/21 and C-275/21, EU:C:2022:565, paragraph 73 and the case-law cited).  
49      Under the principle of sincere cooperation laid down in Article 4(3) TEU it is for the courts of the Member States to ensure judicial protection of a person’s rights under EU law. In addition, Article 19(1) TEU requires Member States to provide remedies sufficient to ensure effective judicial protection in the fields covered by EU law (judgment of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraph 57).  
50      In particular, when the Member States set out detailed procedural rules for legal actions intended to ensure the protection of rights conferred by Regulation 2016/679, they must ensure compliance with the right to an effective remedy and to a fair trial, enshrined in Article 47 of the Charter, which constitutes a reaffirmation of the principle of effective judicial protection (see, by analogy, judgment of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraph 59).  
51      Thus, the Member States must ensure that the practical arrangements for the exercise of the remedies provided for in Article 77(1), Article 78(1) and Article 79(1) of Regulation 2016/679 do not disproportionately affect the right to an effective remedy before a court or tribunal referred to in Article 47 of the Charter (see, to that effect, judgment of 27 September 2017,   
Puškár  
, C-73/16, EU:C:2017:725, paragraph 76).  
52      In the present case, it is apparent from the order for reference that the system of remedies under Hungarian law is designed in such a way that the remedies provided for in Article 78(1) and Article 79(1) of Regulation 2016/679 are independent of each other. The referring court states that, pursuant to that law, it is not bound by the decision given by the court seised of an action brought on the basis of Article 79(1) of that regulation, even though the facts of which those courts are seised are the same.  
53      Therefore, it cannot be ruled out that the decisions given by those two courts might be contradictory, with one finding that the provisions of Regulation 2016/679 have been infringed and the other that there has been no such infringement.  
54      In that case, first, the existence of two contradictory decisions would call into question the objective, set out in recital 10 of that regulation, of ensuring a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data throughout the European Union.  
55      The protection granted pursuant to a decision given to dispose of an action brought on the basis of Article 79(1) of that regulation, finding that that regulation’s provisions have been infringed, would not be consistent with a second judicial decision resulting from an action brought on the basis of Article 78(1) of that regulation that has the opposite outcome.  
56      Second, the result of this would be a weakening of the protection of natural persons with regard to the processing of their personal data, since such an inconsistency would create a situation of legal uncertainty.  
57      Having regard to all of the foregoing, the answer to the questions referred is that Article 77(1), Article 78(1) and Article 79(1) of Regulation 2016/679, read in the light of Article 47 of the Charter, must be interpreted as permitting the remedies provided for in Article 77(1) and Article 78(1) of that regulation, on the one hand, and Article 79(1) thereof, on the other, to be exercised concurrently with and independently of each other. It is for the Member States, in accordance with the principle of procedural autonomy, to lay down detailed rules as regards the relationship between those remedies in order to ensure the effective protection of the rights guaranteed by that regulation and the consistent and homogeneous application of its provisions, as well as the right to an effective remedy before a court or tribunal as referred to in Article 47 of the Charter.  
   
Costs  
58      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
Article 77(1), Article 78(1) and Article 79(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), read in the light of Article 47 of the Charter of Fundamental Rights of the European Union,  
must be interpreted as permitting the remedies provided for in Article 77(1) and Article 78(1) of that regulation, on the one hand, and Article 79(1) thereof, on the other, to be exercised concurrently with and independently of each other. It is for the Member States, in accordance with the principle of procedural autonomy, to lay down detailed rules as regards the relationship between those remedies in order to ensure the effective protection of the rights guaranteed by that regulation and the consistent and homogeneous application of its provisions, as well as the right to an effective remedy before a court or tribunal as referred to in Article 47 of the Charter of Fundamental Rights.  
Signatures  
\*      Language of the case: Hungarian.  
   
  
  
  
  
Disclaimer

ID: b6e3894b-f1b2-43d5-844e-c4f9dc23c768

Judgment of 20 May 2003, C-465/00 (  
Österreichischer Rundfunk and Others  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legal obligation   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
General data protection law   
 >   
Chapter II - Principles   
 >   
Data minimisation   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legal obligation   
   
JUDGMENT OF THE COURT  
20 May 2003 (1)  
(Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Protection of private life - Disclosure of data on the income of employees of bodies subject to control by the Rechnungshof)  
In Joined Cases C-465/00, C-138/01 and C-139/01,  
REFERENCES to the Court under Article 234 EC by the Verfassungsgerichtshof (C-465/00) and the Oberster Gerichtshof (C-138/01 and C-139/01) (Austria) for preliminary rulings in the proceedings pending before those courts between   
 Rechnungshof (C-465/00)  
and  
 Österreichischer Rundfunk,  
Wirtschaftskammer Steiermark,  
Marktgemeinde Kaltenleutgeben,  
Land Niederösterreich,  
Österreichische Nationalbank,  
Stadt Wiener Neustadt,  
Austrian Airlines, Österreichische Luftverkehrs-AG,  
and between   
 Christa Neukomm (C-138/01),  
Joseph Lauermann (C-139/01)  
and  
 Österreichischer Rundfunk,  
on the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31),  
THE COURT,  
composed of: G.C. Rodríguez Iglesias, President, J.-P. Puissochet, M. Wathelet (Rapporteur) and R. Schintgen (Presidents of Chambers), C. Gulmann, D.A.O. Edward, A. La Pergola, P. Jann, V. Skouris, F. Macken, N. Colneric, S. von Bahr and J.N. Cunha Rodrigues, Judges,  
Advocate General: A. Tizzano,  
Registrar: M.-F. Contet, Principal Administrator,  
after considering the written observations submitted on behalf of:  
-    the Rechnungshof, by F. Fiedler, acting as Agent (C-465/00),   
-    Österreichischer Rundfunk, by P. Zöchbauer, Rechtsanwalt (C-465/00),   
-    Wirtschaftskammer Steiermark, by P. Mühlbacher and B. Rupp, acting as Agents (C-465/00),   
-    Marktgemeinde Kaltenleutgeben, by F. Nistelberger, Rechtsanwalt (C-465/00),   
-    Land Niederösterreich, by E. Pröll, C. Kleiser and L. Staudigl, acting as Agents (C-465/00),   
-    Österreichische Nationalbank, by K. Liebscher and G. Tumpel-Gugerell, acting as Agents (C-465/00),   
-    Stadt Wiener Neustadt, by H. Linhart, acting as Agent (C-465/00),   
-    Austrian Airlines, Österreichische Luftverkehrs-AG, by H. Jarolim, Rechtsanwalt (C-465/00),   
-    the Austrian Government, by H. Dossi, acting as Agent (C-465/00, C-138/01 and C-139/01),   
-    the Danish Government, by J. Molde, acting as Agent (C-465/00),   
-    the Italian Government, by U. Leanza, acting as Agent, assisted by D. Del Gaizo, avvocato dello Stato (C-465/00) and O. Fiumara, avvocato generale dello Stato (C-138/01 and C-139/01),   
-    the Netherlands Government, by H.G. Sevenster, acting as Agent (C-465/00, C-138/01 and C-139/01),   
-    the Finnish Government, by E. Bygglin, acting as Agent (C-465/00),   
-    the Swedish Government, by A. Kruse, acting as Agent (C-465/00, C-138/01 and C-139/01),   
-    the United Kingdom Government, by R. Magrill, acting as Agent, and J. Coppel, Barrister (C-465/00, C-138/01 and C-139/01),   
-    the Commission of the European Communities, by U. Wölker and X. Lewis, acting as Agents (C-465/00, C-138/01 and C-139/01),   
   
having regard to the Report for the Hearing,  
after hearing the oral observations of Marktgemeinde Kaltenleutgeben, represented by F. Nistelberger; Land Niederösterreich, represented by C. Kleiser; Österreichische Nationalbank, represented by B. Gruber, Rechtsanwalt; Austrian Airlines, Österreichische Luftverkehrs-AG, represented by H. Jarolim; the Austrian Government, represented by W. Okresek, acting as Agent; the Italian Government, represented by M. Fiorilli, avvocato dello Stato; the Netherlands Government, represented by J. van Bakel, acting as Agent; the Finnish Government, represented by T. Pynnä, acting as Agent; the Swedish Government, represented by A. Kruse and B. Hernqvist, acting as Agent; and the Commission, represented by U. Wölker and C. Docksey, acting as Agent, at the hearing on 18 June 2002,  
after hearing the Opinion of the Advocate General at the sitting on 14 November 2002,  
gives the following  
Judgment  
1.     By orders of 12 December 2000 and 28 and 14 February 2001, the first of which was received at the Court on 28 December 2000 and the other two on 27 March 2001, the Verfassungsgerichtshof (Constitutional Court) (C-465/00) and the Oberster Gerichtshof (Supreme Court) (C-138/01 and C-139/01) each referred to the Court under Article 234 EC two questions, formulated in substantially the same way, on the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).   
2.     Those questions were raised in proceedings between, first, the Rechnungshof (Court of Audit) and a large number of bodies subject to its control and, second, Ms Neukomm and Mr Lauermann and their employer Österreichischer Rundfunk (ÖRF), a broadcasting organisation governed by public law, concerning the obligation of public bodies subject to control by the Rechnungshof to communicate to it the salaries and pensions exceeding a certain level paid by them to their employees and pensioners together with the names of the recipients, for the purpose of drawing up an annual report to be transmitted to the Nationalrat, the Bundesrat and the Landtage (the lower and upper chambers of the Federal Parliament and the provincial assemblies) and made available to the general public (the Report).   
 Legal context  
National provisions  
   
3.     Under Paragraph 8 of the Bundesverfassungsgesetz über die Begrenzung von Bezügen öffentlicher Funktionäre (Federal constitutional law on the limitation of salaries of public officials, BGBl. I 1997/64, as amended, the BezBegrBVG):   
1.    Bodies subject to control by the Rechnungshof must, within the first three months of each second calendar year, inform the Rechnungshof of the salaries or pensions of persons who in at least one of the two previous calendar years drew salaries or pensions greater annually than 14 times 80% of the monthly reference amount under Paragraph 1 [for 2000, 14 times EUR 5 887.87]. The bodies must also state the salaries and pensions of persons who draw an additional salary or pension from a body subject to audit by the Rechnungshof. Persons who draw a salary or pension from two or more bodies subject to control by the Rechnungshof must inform the bodies of this. If this duty of disclosure is not complied with by the body, the Rechnungshof must inspect the relevant documents and draw up its report on the basis thereof.  
2.    In the application of subparagraph 1, social benefits and benefits in kind are also to be taken into account, unless they are benefits from sickness or accident insurance or on the basis of comparable provisions of   
Land  
 law. Where several salaries or pensions are paid by bodies subject to control by the Rechnungshof, they are to be aggregated.  
3.    The Rechnungshof shall summarise that information - for each year separately - in a report. The report shall include all persons whose total yearly salaries and pensions from bodies subject to control by the Rechnungshof exceed the amount stated in subparagraph 1. The report shall be transmitted to the Nationalrat, the Bundesrat and the Landtage.  
4.     It appears from the orders of reference that, in the light of the   
travaux préparatoires  
 of the BezBegrBVG, legal commentators deduce from the latter provision that the Report must give the names of the persons concerned and against each name the amount of annual remuneration received.   
5.     The Verfassungsgerichtshof states that, in accordance with the legislature's intention, the Report must be made available to the general public, so as to provide them with comprehensive information. It states that through this information pressure is brought to bear on the bodies concerned to keep salaries at a low level, so that public funds are used thriftily, economically and efficiently.   
6.     The bodies subject to audit by the Rechnungshof are the Federation, the   
Länder  
 (Federal provinces), large municipalities and - where a reasoned request has been made by the government of a   
Land  
 - municipalities with fewer than 20 000 inhabitants, associations of municipalities, social security institutions, statutory professional bodies, Österreichischer Rundfunk, institutions, funds and foundations managed by organs of the Federation or the   
Länder  
 or by persons appointed by them for that purpose, and undertakings managed by the Federation, a   
Land  
 or a municipality or (alone or jointly with other bodies subject to control by the Rechnungshof) controlled through a company-law holding of not less than 50% or otherwise.   
Community legislation  
7.     Recitals 5 to 9 in the preamble to Directive 95/46 show that it was adopted on the basis of Article 100a of the EC Treaty (now, after amendment, Article 95 EC) to encourage the free movement of personal data through the harmonisation of the laws, regulations and administrative provisions of the Member States on the protection of individuals with regard to the processing of such data.   
8.     According to Article 1 of Directive 95/46:   
1.    In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.  
2.    Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.  
9.     In this connection, recitals 2 and 3 of Directive 95/46 read as follows:   
(2)    Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;   
(3)    Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.   
10.     Recital 10 of Directive 95/46 adds:   
(10)    Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; ...   
 11.     Under Article 6(1) of Directive 95/46, personal data (that is, in accordance with Article 2(a), any information relating to an identified or identifiable natural person) must be:   
(a)    processed fairly and lawfully;   
(b)    collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ...   
(c)    adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;   
...  
12.     Article 2(b) of Directive 95/46 defines processing of personal data as:   
any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.  
13.     Under Article 7 of Directive 95/46, personal data may be processed only if one of the six conditions it sets out is satisfied, and in particular if:   
(c)    processing is necessary for compliance with a legal obligation to which the controller is subject; or   
...  
(e)    processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ... to whom the data are disclosed.   
14.     According to recital 72 of Directive 95/46, the directive allows for the principle of public access to official documents to be taken into account when implementing the principles set out in the directive.   
15.     As regards the scope of Directive 95/46, Article 3(1) provides that it is to apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. However, under Article 3(2), the directive shall not apply to the processing of personal data:   
 -    in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law;   
-    by a natural person in the course of a purely personal or household activity.   
16.     In addition, Article 13 of Directive 95/46 authorises Member States to derogate from certain of its provisions, in particular Article 6(1), where this is necessary to safeguard   
inter alia  
 an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters (Article 13(1)(e)) or a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in certain cases referred to, including that in subparagraph (e) (Article 13(1)(f)).   
 The main proceedings and the questions referred for preliminary rulings  
Case C-465/00  
17.     Differences of opinion as to the interpretation of Paragraph 8 of the BezBegrBVG arose between the Rechnungshof and a large number of bodies under its control with respect to salaries and pensions paid in 1998 and 1999.   
18.     The defendants in the main proceedings, which include local and regional authorities (a   
Land  
 and two municipalities), public undertakings, some of which are in competition with other Austrian or foreign undertakings not subject to control by the Rechnungshof, and a statutory professional body (Wirtschaftskammer Steiermark), did not communicate the data on the income of the employees in question, or communicated the data, to a greater or lesser extent, in anonymised form. They refused access to the relevant documents or made access subject to conditions which the Rechnungshof did not accept. The Rechnungshof therefore brought proceedings before the Verfassungsgerichtshof pursuant to Article 126a of the Bundes-Verfassungsgesetz (Federal Constitutional Law), which gives that court jurisdiction to rule on differences of opinion concerning the interpretation of the statutory provisions governing the jurisdiction of the Rechnungshof.   
19.     The Rechnungshof infers from Paragraph 8 of the BezBegrBVG an obligation to list in the Report the names of the persons concerned and show their annual income. The defendants in the main proceedings take a different view and consider that they are not obliged to communicate personal data relating to that income, such as the names or positions of the persons concerned, with an indication of the emoluments received by them. They rely principally on Directive 95/46, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 (the Convention), which guarantees respect for private life, and on the argument that the obligation of publicity creates a barrier to the movement of workers, contrary to Article 39 EC.   
20.     The Verfassungsgerichtshof wishes essentially to know whether Paragraph 8 of the BezBegrBVG, as interpreted by the Rechnungshof, is compatible with Community law, so that it can interpret it consistently with Community law or declare it (partly) inapplicable, as the case may be.   
21.     It points out, in this connection, that the provisions of Directive 95/46, in particular Articles 6(1)(b) and (c) and 7(c) and (e), must be interpreted in the light of Article 8 of the Convention. It considers that comprehensive information for the public, as intended by the national legislature with respect to the income of employees of bodies subject to control by the Rechnungshof whose annual remuneration exceeds a certain threshold (ATS 1 127 486 in 1999 and ATS 1 120 000 in 1998), has to be regarded as an interference with private life, which can be justified under Article 8(2) of the Convention only if that information contributes to the economic well-being of the country. An interference with fundamental rights cannot be justified by the existence of a mere public interest in information. The court doubts that the disclosure, by means of the Report, of data on personal income promotes the economic well-being of the country. In any event, it constitutes a disproportionate interference with private life. The audit carried out by the Rechnungshof is indubitably sufficient to ensure the proper use of public funds.   
22.     The national court is also uncertain as to whether the scope of Community law varies according to the nature of the body which is required to contribute to the disclosure of the individual income of some of its employees.   
23.     In those circumstances, the Verfassungsgerichtshof decided to stay proceedings and refer the following two questions to the Court for a preliminary ruling:   
1.    Are the provisions of Community law, in particular those on data protection, to be interpreted as precluding national legislation which requires a State body to collect and transmit data on income for the purpose of publishing the names and income of employees of:   
    (a)    a regional or local authority,   
    (b)    a broadcasting organisation governed by public law,   
    (c)    a national central bank,   
    (d)    a statutory representative body,   
     (e)    a partially State-controlled undertaking which is operated for profit?   
2.    If the answer to at least part of the above question is in the affirmative:   
    Are the provisions precluding such national legislation directly applicable, in the sense that the persons obliged to make disclosure may rely on them to prevent the application of contrary national provisions?   
Cases C-138/01 and C-139/01  
24.     Ms Neukomm and Mr Lauermann, who are employees of ÖRF, a body subject to control by the Rechnungshof, brought proceedings in the Austrian courts for interim orders to prevent ÖRF from acceding to the Rechnungshof's request to communicate data.   
25.     The applications for interim orders were dismissed at first instance. The Arbeits- und Sozialgericht Wien (Labour and Social Court, Vienna) (Austria) (C-138/01), distinguishing between the transmission of the data to the Rechnungshof and its inclusion in the Report, considered that the Report had to be anonymous, while the mere transmission of the data to the Rechnungshof, even including names, did not infringe Article 8 of the Convention or Directive 95/46. The Landesgericht St Pölten (Regional Court, St Pölten) (Austria) (C-139/01), on the other hand, held that the inclusion of data with names in the Report was lawful, since an anonymised report would not enable the Rechnungshof to exercise adequate control.   
26.     The Oberlandesgericht Wien (Higher Regional Court, Vienna) (Austria) upheld on appeal the dismissal of the applications for interim orders by the courts at first instance. While stating, in connection with Case C-138/01, that in communicating the data in question the employer is merely performing a task imposed on him by law and that the subsequent processing of the data by the Rechnungshof is not carried out under the control of the employer, the Oberlandesgericht held, in the context of Case C-139/01, that Paragraph 8 of the BezBegrBVG was consistent with fundamental rights and with Directive 95/46, even in the case of a list by name of the persons concerned.   
27.     Ms Neukomm and Mr Lauermann appealed on a point of law (  
Revision  
) to the Oberster Gerichtshof.   
28.     The Oberster Gerichtshof, referring to the reference for a preliminary ruling in Case C-465/00 and adopting the points of law raised by the Verfassungsgerichtshof, decided to stay proceedings and refer the following two questions to the Court, using the same wording in Cases C-138/01 and C-139/01:   
 1.    Are the provisions of Community law, in particular those on data protection (Articles 1, 2, 6, 7 and 22 of Directive 95/46/EC in conjunction with Article 6 (formerly Article F) of the Treaty on European Union and Article 8 of the Convention), to be interpreted as precluding national legislation which requires a public broadcasting organisation, as a legal body, to communicate, and a State body to collect and transmit, data on income for the purpose of publishing the names and income of employees of a broadcasting organisation governed by public law?   
2.    If the Court of Justice of the European Communities answers the above question in the affirmative:   
    Are the provisions precluding national legislation of the kind described above directly applicable, in the sense that an organisation obliged to make disclosure may rely on them to prevent the application of contrary national legislation, and may not therefore rely on an obligation under national law against the employees concerned by the disclosure?   
29.     By order of the President of the Court of 17 May 2001, Cases C-138/01 and C-139/01 were joined for the purposes of the written procedure, the oral procedure and judgment. Case C-465/00 and Cases C-138/01 and C-139/01 should also be joined for the purposes of judgment.   
30.     The questions put by the Verfassungsgerichtshof and the Oberster Gerichtshof are essentially the same, and should therefore be examined together.   
 Applicability of Directive 95/46  
31.     To answer the questions as put would presuppose that Directive 95/46 is applicable in the main proceedings. That applicability is, however, disputed before the Court. This point must be decided as a preliminary issue.   
Observations submitted to the Court  
32.     The defendants in the main proceedings in Case C-465/00 consider essentially that the control activity exercised by the Rechnungshof falls within the scope of Community law and hence of Directive 95/46. In particular, in that it relates to the remuneration received by the employees of the bodies concerned, that activity touches aspects covered by Community provisions in social matters, such as Articles 136 EC, 137 EC and 141 EC, Council Directive 76/207/EEC of 9 February 1976 on the implementation of the principle of equal treatment for men and women as regards access to employment, vocational training and promotion, and working conditions (OJ 1976 L 39, p. 40), and Council Regulation (EEC) No 1408/71 of 14 June 1971 on the application of social security schemes to employed persons, to self-employed persons and to members of their families moving within the Community, as amended and updated by Council Regulation (EC) No 118/97 of 2 December 1996 (OJ 1997 L 28, p. 1).   
33.     They further submit that the control exercised by the Rechnungshof, first, affects the possibility for employees of the bodies concerned to seek employment in another Member State, because of the publicity attaching to their salaries which limits their power of negotiation with foreign companies, and, second, deters nationals of other Member States from seeking employment with the bodies subject to that control.   
34.     Austrian Airlines, Österreichische Luftverkehrs-AG states that the interference with the freedom of movement of workers is particularly serious in its case because it competes with companies of other Member States which are not subject to such control.   
35.     The Rechnungshof and the Austrian and Italian Governments, and to a certain extent the Commission, on the other hand, consider that Directive 95/46 is not applicable in the main proceedings.   
36.     According to the Rechnungshof and the Austrian and Italian Governments, the control activity referred to in Paragraph 8 of the BezBegrBVG, which pursues objectives in the public interest in the field of public accounts, does not fall within the scope of Community law.   
37.     After observing that the directive, which was adopted on the basis of Article 100a of the Treaty, has the objective of establishing the internal market, an aspect of which is the protection of the right to privacy, the Rechnungshof and the Austrian and Italian Governments submit that the control in question is not such as to obstruct the freedom of movement of workers, since it does not in any way prevent the employees of the bodies concerned from going to work in another Member State or those of other Member States from working for those bodies. In any event, the link between the control activity and the freedom of movement of workers, even supposing that workers do seek to avoid working for a body subject to control by the Rechnungshof because of the publicity attaching to the salaries received, is too uncertain and indirect to constitute an infringement of freedom of movement and thereby to allow a link to be made with Community law.   
38.     The Commission adopts a similar position. At the hearing, it nevertheless submitted that the collection of data by the bodies subject to control by the Rechnungshof with a view to communication to the latter and inclusion in the report is itself within the scope of Directive 95/46. Collection serves not only the function of auditing but also, primarily, the payment of remuneration, which constitutes an activity covered by Community law, having regard to the existence of various relevant social provisions in the Treaty, such as Article 141 EC, and to the possible effect of that activity on the freedom of movement of workers.   
Findings of the Court  
39.     Directive 95/46, adopted on the basis of Article 100a of the Treaty, is intended to ensure the free movement of personal data between Member States through the harmonisation of national provisions on the protection of individuals with regard to the processing of such data. Article 1, which defines the object of the directive, provides in paragraph 2 that Member States may neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection of the fundamental rights and freedoms of natural persons, in particular their private life, with respect to the processing of that data.   
40.     Since any personal data can move between Member States, Directive 95/46 requires in principle compliance with the rules for protection of such data with respect to any processing of data as defined by Article 3.   
41.     It may be added that recourse to Article 100a of the Treaty as legal basis does not presuppose the existence of an actual link with free movement between Member States in every situation referred to by the measure founded on that basis. As the Court has previously held (see Case C-376/98   
Germany  
 v   
Parliament and Council  
 [2000] ECR I-8419, paragraph 85, and Case C-491/01   
British American Tobacco (Investments) and Imperial Tobacco  
 [2002] ECR I-11453, paragraph 60), to justify recourse to Article 100a of the Treaty as the legal basis, what matters is that the measure adopted on that basis must actually be intended to improve the conditions for the establishment and functioning of the internal market. In the present case, that fundamental attribute was never in dispute before the Court with respect to the provisions of Directive 95/46, in particular those in the light of which the national court raises the question of the compatibility of the national legislation in question with Community law.   
42.     In those circumstances, the applicability of Directive 95/46 cannot depend on whether the specific situations at issue in the main proceedings have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty, in particular, in those cases, the freedom of movement of workers. A contrary interpretation could make the limits of the field of application of the directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations.   
43.     Moreover, the applicability of Directive 95/46 to situations where there is no direct link with the exercise of the fundamental freedoms of movement guaranteed by the Treaty is confirmed by the wording of Article 3(1) of the directive, which defines its scope in very broad terms, not making the application of the rules on protection depend on whether the processing has an actual connection with freedom of movement between Member States. That is also confirmed by the exceptions in Article 3(2), in particular those concerning the processing of personal data in the course of an activity ... provided for by Titles V and VI of the Treaty on European Union or in the course of a purely personal or household activity. Those exceptions would not, at the very least, be worded in that way if the directive were applicable exclusively to situations where there is a sufficient link with the exercise of freedoms of movement.   
44.     The same observation may be made with regard to the exceptions in Article 8(2) of Directive 95/46, which concern the processing of specific categories of data, in particular those in Article 8(2)(d), which refers to processing carried out by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim.   
45.     Finally, the processing of personal data at issue in the main proceedings does not fall within the exception in the first indent of Article 3(2) of Directive 95/46. That processing does not concern the exercise of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union. Nor is it a processing operation concerning public security, defence, State security or the activities of the State in areas of criminal law.   
46.     The purposes set out in Articles 7(c) and (e) and 13(e) and (f) of Directive 95/46 show, moreover, that it is intended to cover instances of data processing such as those at issue in the main proceedings.   
47.     It must therefore be considered that Directive 95/46 is applicable to the processing of personal data provided for by legislation such as that at issue in the main proceedings.   
 The first question  
48.     By their first question, the national courts essentially ask whether Directive 95/46 is to be interpreted as precluding national legislation such as that at issue in the main proceedings which requires a State control body to collect and communicate, for purposes of publication, data on the income of persons employed by the bodies subject to that control, where that income exceeds a certain threshold.   
Observations submitted to the Court  
49.     The Danish Government considers that Directive 95/46 does not, strictly speaking, govern the right of third parties to obtain access to documents on request. In particular, Article 12 of the directive refers only to the right of any person to obtain data concerning him. According to the Government, the protection of personal data which appear not to be sensitive must give way to the principle of transparency, which holds an essential place in the Community legal order. The Danish Government, with the Swedish Government, observes in this respect that, according to recital 72 of the directive, the principle of public access to official documents may be taken into account when implementing the directive.   
50.     The Rechnungshof, the Austrian, Italian, Netherlands, Finnish and Swedish Governments and the Commission consider that the national provisions at issue in the main proceedings are compatible with Directive 95/46, by reason, generally, of the wide discretion the Member States have in implementing it, in particular where a task in the public interest provided for by law is to be carried out, under Articles 6(b) and (c) and 7(c) or (e) of the directive. Both the principles of transparency and of the proper management of public funds and the prevention of abuses are relied on in this respect.   
51.     Those objectives in the public interest can justify an interference with private life, protected by Article 8(2) of the Convention, if it is in accordance with the law, is necessary in a democratic society for the pursuit of legitimate aims, and is not disproportionate to the objective pursued.   
52.     The Austrian Government notes in particular that, when reviewing proportionality, the extent to which the data affect private life must be taken into account. Data relating to personal intimacy, health, family life or sexuality must therefore be protected more strongly than data relating to income and taxes, which, while also personal, concern personal identity to a lesser extent and are thereby less sensitive (see, to that effect,   
Fressoz and Roire v. France  
 [GC], no. 29183/95, § 65, ECHR 1999-I).   
53.     The Finnish Government likewise considers that protection of private life is not absolute. Data relating to a person acting in the course of a public office or public functions relating thereto do not fall within the protection of private life.   
54.     The Italian Government submits that data such as that at issue in the main proceedings are already by their nature public in most Member States, since they are visible from salary scales or remuneration brackets laid down by statute, regulation or collective agreements. In those circumstances, it is not contrary to the principle of proportionality to provide for diffusion of that data with the identities of the various people in receipt of the salaries in question. That diffusion, being thus intended to clarify a situation that is already apparent from data available to the public, constitutes the minimum measure which would ensure realisation of the objectives of transparency and sound administration.   
 55.     The Netherlands Government adds, however, that the national courts must ascertain, for each public body concerned, whether the objective of public interest can be attained by processing the personal data in a way that interferes less with the private lives of the persons concerned.   
56.     The United Kingdom Government submits that, in answering the first question, the provisions of the Charter of Fundamental Rights of the European Union, proclaimed in Nice on 18 December 2000 (OJ 2000 C 364, p. 1), to which the Verfassungsgericht briefly refers, are of no relevance.   
57.     In Cases C-138/01 and C-139/01, the Commission questions whether, in the context of examining proportionality under Article 6(1)(b) of Directive 95/46, it might not suffice for attaining the objective pursued by the BezBegrBVG to transmit the data in an anonymised form, for example by indicating the function of the person concerned rather than his name. Even if it is admitted that the Rechnungshof needs details of names in order to carry out a more exact check, it is questionable whether the inclusion of that data in the Report, giving the name of the person concerned, is really necessary for performing that check, especially as the Report is not only submitted to the parliamentary assemblies but must also be widely published.   
58.     Moreover, the Commission observes that under Article 13 of Directive 95/46 the Member States may   
inter alia  
 derogate from Article 6(1)(b) of the directive in order to safeguard a number of objectives in the public interest, in particular an important economic or financial interest of a Member State (Article 13(1)(e)). However, in the Commission's view, the derogating measures must also comply with the principle of proportionality, which calls for the same considerations as those stated in the preceding paragraph with reference to Article 6(1)(b) of the directive.   
59.     The defendants in the main proceedings in Case C-465/00 consider that the national legislation at issue is incompatible with Article 6(1)(b) and (c) of Directive 95/46 and cannot be justified under Article 7(c) or (e) of the directive, since it constitutes an interference which is not justified under Article 8(2) of the Convention, and is in any event disproportionate. The audit performed by the Rechnungshof is sufficient to guarantee the thrifty use of public funds.   
60.     More particularly, it has not been shown that publication of the names and the amount of the income of all persons employed by public bodies where that amount exceeds a certain level constitutes a measure aimed at the economic well-being of the country. The aim of the legislature was to exert pressure on the bodies in question to maintain salaries at a low level. The defendants also submit that that measure is aimed, in the present case, at persons who for the most part are not public figures.   
61.     Moreover, even if the drawing up by the Rechnungshof of a report containing personal data on income intended for public debate were to be regarded as an interference with private life justified under Article 8(2) of the Convention, Land Niederösterreich and ÖRF consider that that measure also violates Article 14 of the Convention. Persons receiving the same income are treated unequally, depending on whether or not they are employed by a body subject to control by the Rechnungshof.   
62.     ÖRF points out a further example of unequal treatment that cannot be justified under Article 14 of the Convention. Among the employees of bodies subject to control by the Rechnungshof, only those whose income exceeds the threshold fixed in Paragraph 8 of the BezBegrBVG have to suffer an interference with their private life. If the legislature attaches real importance to the reasonableness of the remuneration received by the employees of certain bodies, it is then necessary to publish the income of all employees, regardless of its amount.   
63.     Finally, ÖRF, Marktgemeinde Kaltenleutgeben and Austrian Airlines, Österreichische Luftverkehrs-AG submit that the wording of Paragraph 8 of the BezBegrBVG lends itself to an interpretation consistent with Community law, under which the salaries in question are required to be communicated to the Rechnungshof and included in the Report only in anonymised form. That interpretation should prevail, as it resolves the contradiction between that provision and Directive 95/46.   
Findings of the Court  
64.     It should be noted, to begin with, that the data at issue in the main proceedings, which relate both to the monies paid by certain bodies and the recipients, constitute personal data within the meaning of Article 2(a) of Directive 95/46, being information relating to an identified or identifiable natural person. Their recording and use by the body concerned, and their transmission to the Rechnungshof and inclusion by the latter in a report intended to be communicated to various political institutions and widely diffused, constitute processing of personal data within the meaning of Article 2(b) of the directive.   
65.     Under Directive 95/46, subject to the exceptions permitted under Article 13, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, second, with one of the criteria for making data processing legitimate listed in Article 7.   
66.     More specifically, the data must be collected for specified, explicit and legitimate purposes (Article 6(1)(b) of Directive 95/46) and must be adequate, relevant and not excessive in relation to those purposes (Article 6(1)(c)). In addition, under Article 7(c) and (e) of the directive respectively, the processing of personal data is permissible only if it is necessary for compliance with a legal obligation to which the controller is subject or is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ... to whom the data are disclosed.   
67.     However, under Article 13(e) and (f) of the directive, the Member States may derogate   
inter alia  
 from Article 6(1) where this is necessary to safeguard respectively an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters or a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in particular cases including that referred to in subparagraph (e).   
68.     It should also be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures (see,   
inter alia  
, Case C-274/99 P   
Connolly  
 v   
Commission  
 [2001] ECR I-1611, paragraph 37).   
69.     Those principles have been expressly restated in Article 6(2) EU, which states that [t]he Union shall respect fundamental rights, as guaranteed by the [Convention] and as they result from the constitutional traditions common to the Member States, as general principles of Community law.   
70.     Directive 95/46 itself, while having as its principal aim to ensure the free movement of personal data, provides in Article 1(1) that Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Several recitals in its preamble, in particular recitals 10 and 11, also express that requirement.   
71.     In this respect, it is to be noted that Article 8 of the Convention, while stating in paragraph 1 the principle that the public authorities must not interfere with the right to respect for private life, accepts in paragraph 2 that such an interference is possible where it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.   
72.     So, for the purpose of applying Directive 95/46, in particular Articles 6(1)(c), 7(c) and (e) and 13, it must be ascertained, first, whether legislation such as that at issue in the main proceedings provides for an interference with private life, and if so, whether that interference is justified from the point of view of Article 8 of the Convention.   
Existence of an interference with private life  
 73.     First of all, the collection of data by name relating to an individual's professional income, with a view to communicating it to third parties, falls within the scope of Article 8 of the Convention. The European Court of Human Rights has held in this respect that the expression private life must not be interpreted restrictively and that there is no reason of principle to justify excluding activities of a professional ... nature from the notion of private life (see,   
inter alia  
,   
Amann v. Switzerland  
 [GC], no. 27798/95, § 65, ECHR 2000-II and   
Rotaru v. Romania  
 [GC], no. 28341/95, § 43, ECHR 2000-V).   
74.     It necessarily follows that, while the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life, the communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of Article 8 of the Convention.   
75.     To establish the existence of such an interference, it does not matter whether the information communicated is of a sensitive character or whether the persons concerned have been inconvenienced in any way (see, to that effect,   
Amann v. Switzerland  
, § 70). It suffices to find that data relating to the remuneration received by an employee or pensioner have been communicated by the employer to a third party.   
Justification of the interference  
76.     An interference such as that mentioned in paragraph 74 above violates Article 8 of the Convention unless it is in accordance with the law, pursues one or more of the legitimate aims specified in Article 8(2), and is necessary in a democratic society for achieving that aim or aims.   
77.     It is common ground that the interference at issue in the main proceedings is in accordance with Paragraph 8 of the BezBegrBVG. However, the question arises whether that paragraph is formulated with sufficient precision to enable the citizen to adjust his conduct accordingly, and so complies with the requirement of foreseeability laid down in the case-law of the European Court of Human Rights (see,   
inter alia  
,   
Rekvényi v. Hungary  
 [GC], no. 25390/94, § 34, ECHR 1999-III).   
78.     In this respect, Paragraph 8(3) of the BezBegrBVG states that the report drawn up by the Rechnungshof is to include all persons whose total yearly salaries and pensions from bodies ... exceed the amount stated in subparagraph 1, without expressly requiring the names of the persons concerned to be disclosed in relation to the income they receive. According to the orders for reference, it is legal commentators who, on the basis of the   
travaux préparatoires  
, interpret the constitutional law in that way.   
79.     It is for the national courts to ascertain whether the interpretation to the effect that Paragraph 8(3) of the BezBegrBVG requires disclosure of the names of the persons concerned in relation to the income received complies with the requirement of foreseeability referred to in paragraph 77 above.   
80.     However, that question need not arise until it has been determined whether such an interpretation of the national provision at issue is consistent with Article 8 of the Convention, as regards its required proportionality to the aims pursued. That question will be examined below.   
81.     It appears from the order for reference in Case C-465/00 that the objective of Paragraph 8 of the BezBegrBVG is to exert pressure on the public bodies concerned to keep salaries within reasonable limits. The Austrian Government observes, more generally, that the interference provided for by that provision is intended to guarantee the thrifty and appropriate use of public funds by the administration. Such an objective constitutes a legitimate aim within the meaning both of Article 8(2) of the Convention, which mentions the economic well-being of the country, and Article 6(1)(b) of Directive 95/46, which refers to specified, explicit and legitimate purposes.   
82.     It must next be ascertained whether the interference in question is necessary in a democratic society to achieve the legitimate aim pursued.   
83.     According to the European Court of Human Rights, the adjective necessary in Article 8(2) of the Convention implies that a pressing social need is involved and that the measure employed is proportionate to the legitimate aim pursued (see,   
inter alia  
, the Gillow v. the United Kingdom judgment of 24 November 1986, Series A no. 109, § 55). The national authorities also enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, § 59).   
84.     The interest of the Republic of Austria in ensuring the best use of public funds, and in particular keeping salaries within reasonable limits, must be balanced against the seriousness of the interference with the right of the persons concerned to respect for their private life.   
85.     On the one hand, in order to monitor the proper use of public funds, the Rechnungshof and the various parliamentary bodies undoubtedly need to know the amount of expenditure on human resources in the various public bodies. In addition, in a democratic society, taxpayers and public opinion generally have the right to be kept informed of the use of public revenues, in particular as regards expenditure on staff. Such information, put together in the Report, may make a contribution to the public debate on a question of general interest, and thus serves the public interest.   
86.     The question nevertheless arises whether stating the names of the persons concerned in relation to the income received is proportionate to the legitimate aim pursued and whether the reasons relied on before the Court to justify such disclosure appear relevant and sufficient.   
87.     It is plain that, according to the interpretation adopted by the national courts, Paragraph 8 of the BezBegrBVG requires disclosure of the names of the persons concerned, in relation to income above a certain level, with respect not only to persons filling posts remunerated by salaries on a published scale, but to all persons remunerated by bodies subject to control by the Rechnungshof. Moreover, such information is not only communicated to the Rechnungshof and via the latter to the various parliamentary bodies, but is also made widely available to the public.   
88.     It is for the national courts to ascertain whether such publicity is both necessary and proportionate to the aim of keeping salaries within reasonable limits, and in particular to examine whether such an objective could not have been attained equally effectively by transmitting the information as to names to the monitoring bodies alone. Similarly, the question arises whether it would not have been sufficient to inform the general public only of the remuneration and other financial benefits to which persons employed by the public bodies concerned have a contractual or statutory right, but not of the sums which each of them actually received during the year in question, which may depend to a varying extent on their personal and family situation.   
89.     With respect, on the other hand, to the seriousness of the interference with the right of the persons concerned to respect for their private life, it is not impossible that they may suffer harm as a result of the negative effects of the publicity attached to their income from employment, in particular on their prospects of being given employment by other undertakings, whether in Austria or elsewhere, which are not subject to control by the Rechnungshof.   
90.     It must be concluded that the interference resulting from the application of national legislation such as that at issue in the main proceedings may be justified under Article 8(2) of the Convention only in so far as the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by the Rechnungshof but also of the names of the recipients of that income is both necessary for and appropriate to the aim of keeping salaries within reasonable limits, that being a matter for the national courts to examine.   
Consequences with respect to the provisions of Directive 95/46  
   
91.     If the national courts conclude that the national legislation at issue is incompatible with Article 8 of the Convention, that legislation is also incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46. Nor could it be covered by any of the exceptions referred to in Article 13 of that directive, which likewise requires compliance with the requirement of proportionality with respect to the public interest objective being pursued. In any event, that provision cannot be interpreted as conferring legitimacy on an interference with the right to respect for private life contrary to Article 8 of the Convention.   
92.     If, on the other hand, the national courts were to consider that Paragraph 8 of the BezBegrBVG is both necessary for and appropriate to the public interest objective being pursued, they would then, as appears from paragraphs 77 to 79 above, still have to ascertain whether, by not expressly providing for disclosure of the names of the persons concerned in relation to the income received, Paragraph 8 of the BezBegrBVG complies with the requirement of foreseeability.   
93.     Finally, it should be noted, in the light of the above considerations, that the national court must also interpret any provision of national law, as far as possible, in the light of the wording and the purpose of the applicable directive, in order to achieve the result pursued by the latter and thereby comply with the third paragraph of Article 249 EC (see Case C-106/89   
Marleasing  
 [1990] ECR I-4135, paragraph 8).   
94.     In the light of all the above considerations, the answer to the first question must be that Articles 6(1)(c) and 7(c) and (e) of Directive 95/46 do not preclude national legislation such as that at issue in the main proceedings, provided that it is shown that the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by the Rechnungshof but also of the names of the recipients of that income is necessary for and appropriate to the objective of proper management of public funds pursued by the legislature, that being for the national courts to ascertain.   
 The second question  
95.     By their second question, the national courts ask whether the provisions of Directive 95/46 which preclude national legislation such as that at issue in the main proceedings are directly applicable, in that they may be relied on by individuals before the national courts to oust the application of that legislation.   
96.     The defendants in the main proceedings in Case C-465/00 and the Netherlands Government consider that Articles 6(1) and 7 of Directive 95/46 fulfil the criteria stated in the Court's case-law for having such direct effect. They are sufficiently precise and unconditional for the bodies required to disclose the data relating to the income of the persons concerned to be able to rely on them to prevent application of the national provisions contrary to those provisions.   
97.     The Austrian Government submits, on the other hand, that the relevant provisions of Directive 95/46 are not directly applicable. In particular, Articles 6(1) and 7 are not unconditional, since their implementation requires the Member States, which have a wide discretion, to adopt special measures to that effect.   
98.     On this point, it should be noted that wherever the provisions of a directive appear, so far as their subject-matter is concerned, to be unconditional and sufficiently precise, they may, in the absence of implementing measures adopted within the prescribed period, be relied on against any national provision which is incompatible with the directive or in so far as they define rights which individuals are able to assert against the State (see,   
inter alia  
, Case 8/81   
Becker  
 [1982] ECR 53, paragraph 25, and Case C-141/00   
Kügler  
 [2002] ECR I-6833, paragraph 51).   
99.     In the light of the answer to the first question, the second question seeks to know whether such a character may be attributed to Article 6(1)(c) of Directive 95/46, under which personal data must be ... adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, and to Article 7(c) or (e), under which personal data may be processed only if   
inter alia  
 processing is necessary for compliance with a legal obligation to which the controller is subject or is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ... to whom the data are disclosed.   
100.     Those provisions are sufficiently precise to be relied on by individuals and applied by the national courts. Moreover, while Directive 95/46 undoubtedly confers on the Member States a greater or lesser discretion in the implementation of some of its provisions, Articles 6(1)(c) and 7(c) or (e) for their part state unconditional obligations.   
101.     The answer to the second question must therefore be that Articles 6(1)(c) and 7(c) and (e) of Directive 95/46 are directly applicable, in that they may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions.   
 Costs  
102.     The costs incurred by the Austrian, Danish, Italian, Netherlands, Finnish, Swedish and United Kingdom Governments and by the Commission, which have submitted observations to the Court, are not recoverable. Since these proceedings are, for the parties to the main proceedings, a step in the proceedings pending before the national courts, the decisions on costs are a matter for those courts.   
   
On those grounds,  
THE COURT,  
in answer to the questions referred to it by the Verfassungsgerichtshof by order of 12 December 2000 and by the Oberster Gerichtshof by orders of 14 and 28 February 2001, hereby rules:  
 1.    Articles 6(1)(c) and 7(c) and (e) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data do not preclude national legislation such as that at issue in the main proceedings, provided that it is shown that the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by the Rechnungshof but also of the names of the recipients of that income is necessary for and appropriate to the objective of proper management of public funds pursued by the legislature, that being for the national courts to ascertain.   
2.    Articles 6(1)(c) and 7(c) and (e) of Directive 95/46 are directly applicable, in that they may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions.   
Rodríguez IglesiasPuissochet Wathelet   
SchintgenGulmann Edward   
La PergolaJann Skouris   
MackenColneric von Bahr   
Cunha Rodrigues   
Delivered in open court in Luxembourg on 20 May 2003.  
R. Grass G.C. Rodríguez Iglesias   
RegistrarPresident   
1: Language of the case: German.   
  
  
  
  
Disclaimer

ID: baedae37-9c74-4cc8-968b-22520d488073

of 27 Oct 2022, C-129/21 (  
Proximus  
)  
E-privacy Directive   
 >   
Directories of subscribers   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Consent   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter II - Principles   
 >   
Accountability   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Responsibility of the controller   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Powers   
   
JUDGMENT OF THE COURT (Fourth Chamber)  
27 October 2022 (\*)  
(Reference for a preliminary ruling – Processing of personal data and protection of privacy in the electronic communications sector – Directive 2002/58/EC – Article 12 – Public telephone directories and directory enquiry services – Subscriber’s consent – Obligations of the provider of directories and of directory enquiry services – Regulation (EU) 2016/679 – Article 17 – Right to erasure (‘right to be forgotten’) – Article 5(2) – Article 24 – Information obligations and responsibility of the controller)  
In Case C-129/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the hof van beroep te Brussel (Court of Appeal, Brussels, Belgium), made by decision of 24 February 2021, received at the Court on 2 March 2021, in the proceedings  
Proximus NV  
v  
Gegevensbeschermingsautoriteit,  
THE COURT (Fourth Chamber),  
composed of C. Lycourgos, President of the Chamber, L.S. Rossi (Rapporteur), J.-C. Bonichot, S. Rodin and O. Spineanu-Matei, Judges,  
Advocate General: A.M. Collins,  
Registrar: M. Ferreira, Principal Administrator,  
having regard to the written procedure and further to the hearing on 9 February 2022,  
after considering the observations submitted on behalf of:  
–        Proximus NV, by P. Craddock and T. de Haan, avocats, and by E. Van Bogget, advocaat,  
–        Gegevensbeschermingsautoriteit, by C. Buggenhoudt, E. Cloots and J. Roets, advocaten,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by E. De Bonis, avvocato dello Stato,  
–        the Latvian Government, by E. Bārdiņš, J. Davidoviča and K. Pommere, acting as Agents,  
–        the Portuguese Government, by P. Barros da Costa, L. Inez Fernandes, M.J. Ramos and C. Vieira Guerra, acting as Agents,  
–        the Romanian Government, by E. Gane and L. Liţu, acting as Agents,  
–        the European Commission, by S.L. Kalėda, H. Kranenborg and P.-J. Loewenthal, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 28 April 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 12(2), read in conjunction with point (f) of the second paragraph of Article 2 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), and of Article 5(2) and Articles 17, 24 and 95 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
2        The request has been made in proceedings between Proximus NV, a company governed by Belgian public law, and the Gegevensbeschermingsautoriteit (Data Protection Authority, Belgium) (‘the DPA’), concerning the decision by which the Geschillenkamer van de Gegevensbeschermingsautoriteit (Litigation Chamber of the DPA; ‘the Litigation Chamber’) ordered Proximus to take remedial action and to pay a fine of EUR 20 000 for infringement of several provisions of the GDPR.  
   
Legal context  
   
European Union law  
   
Directive 95/46/EC  
3        Article 2(h) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) provides:  
‘For the purposes of this Directive:  
…  
(h)      “the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.’  
   
Directive 2002/58  
4        Recitals 10, 17, 38 and 39 of Directive 2002/58 are worded as follows:  
‘(10)      In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. …  
…  
(17)      For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject’s consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an Internet website.  
…  
(38)      Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.  
(39)      The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.’  
5        Article 1 of that directive provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.  
2.      The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.  
…’  
6        Article 2 of Directive 2002/58, entitled ‘Definitions’, provides in point (f) of the second paragraph thereof:  
‘The following definitions shall also apply:  
…  
(f)      “consent” by a user or subscriber corresponds to the data subject’s consent in Directive 95/46/EC’.  
7        Article 12 of that directive, entitled ‘Directories of subscribers’, states:  
‘1.      Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.  
2.      Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.  
3.      Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.  
…’  
   
The GDPR  
8        Recitals 42, 66 and 173 of the GDPR state:  
‘(42)      Where processing is based on the data subject’s consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. … a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.  
…  
(66)      To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject’s request.  
…  
(173)      This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC …, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.’  
9        Article 4(2), (7) and (11) of that regulation is worded as follows:  
‘For the purposes of this Regulation:  
…  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …  
…  
(11)      “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.  
10      Article 5 of the GDPR, entitled ‘Principles relating to processing of personal data’, provides:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
…  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
11      Under Article 6 of the GDPR, entitled ‘Lawfulness of processing’:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
…’  
12      Article 7 of the GDPR, entitled ‘Conditions for consent’, states:  
‘1.      Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.  
…  
3.      The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.  
…’  
13      Article 16 of the GDPR, entitled ‘Right to rectification’, provides:  
‘The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.’  
14      Article 17 of the GDPR, entitled ‘Right to erasure (“right to be forgotten”)’, is worded as follows:  
‘1.      The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:  
…  
(b)      the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;  
…  
(d)      the personal data have been unlawfully processed;  
2.      Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.  
…’  
15      Article 19 of the GDPR, entitled ‘Notification obligation regarding rectification or erasure of personal data or restriction of processing’, provides:  
‘The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.’  
16      Under Article 24 of the GDPR, entitled ‘Responsibility of the controller’:  
‘1.      Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.  
2.      Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.  
…’  
17      Article 94 of the GDPR, entitled ‘Repeal of Directive 95/46/EC’, provides in paragraph 2:  
‘References to the repealed Directive shall be construed as references to this Regulation. …’  
18      Article 95 of the GDPR, entitled ‘Relationship with Directive 2002/58/EC’, provides:  
‘This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the [European] Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.’  
   
Belgian law  
19      Article 133 of the Wet betreffende de elektronische communicatie (Law on electronic communication), of 13 June 2005 (  
Belgisch Staatsblad  
, 20 June 2005, p. 28070), which transposes Article 12 of Directive 2002/58 into Belgian law, is worded as follows:  
‘1.      Providers of a publicly available telephone service shall inform their subscribers free of charge and before including them in a telephone directory or directory enquiry service of:  
1.      the purpose of the telephone directory or of the directory enquiry service;  
2.      the fact that inclusion in the telephone directory or directory enquiry service is free of charge;  
3.      any uses of the telephone directory or of the directory enquiry service other than the retrieval of personal data on the basis of the name of the subscriber and, where appropriate, the place where the subscriber has his or her permanent address or usually resides or the place where the subscriber has his or her principal place of business.  
Only personal data which are relevant for the purpose as communicated in accordance with subparagraph 1 and in respect of which the subscriber in question has indicated that they could be included in the telephone directory or directory enquiry service in question may be included in the telephone directory or directory enquiry service.  
To that end, two separate questions shall be put by the operator to the subscriber:  
1.      whether he or she wishes his or her contact details to be included in the universal directory and in the universal enquiry service;  
2.      whether he or she wishes his or her contact details to be included in other directories or other enquiry services.  
…  
2.      Every subscriber shall have the right to consult personal data concerning him or her under the conditions laid down by, or pursuant to, the Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data).  
Every subscriber shall also have the right to have personal data concerning him or her corrected or withdrawn free of charge from the telephone directory or directory enquiry service in accordance with the procedures and under the conditions laid down by the King, after obtaining the opinion of the Committee for the Protection of Privacy and the Institute.’  
20      Article 45(2) of that law obliges telephone service operators to make the data relating to their subscribers available to providers of public directories. Pursuant to Article 45(3) thereof, those operators are to keep separate the data relating to subscribers who have indicated that they do not wish to be included in a directory so as to allow those subscribers to receive the directory without their data being included therein.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
21      Proximus, a telecommunications service provider in Belgium, also provides publicly available telephone directories and directory enquiry services (‘directories’) in accordance with the provisions of the Law on electronic communication. Those directories contain the name, address and telephone number (‘contact details’) of the subscribers of the various providers of publicly available telephone services (‘operators’). There are other directories that are published by third parties.  
22      The contact details of the subscribers concerned are regularly communicated to Proximus by the operators, with the exception of those subscribers who have expressed the wish not to be included in the directories published by Proximus. In Belgium, the distinction between subscribers who wish to appear in a directory and those who do not leads, in practice, to the assignment of a code in the record of each subscriber, namely ‘NNNNN’ for subscribers whose contact details may appear and ‘XXXXX’ for subscribers whose contact details are to remain confidential. Proximus also supplies the contact details that it receives to another provider of directories.  
23      The complainant is a subscriber of the telephone service operator, Telenet, which is active on the Belgian market. Telenet does not provide directories, rather it supplies the contact details of its subscribers to providers of directories, inter alia to Proximus.  
24      On 13 January 2019, the complainant asked Proximus not to include his contact details in directories published both by Proximus and by third parties. Following that request, Proximus changed that subscriber’s status in its computer system so that his contact details would no longer be made public.  
25      On 31 January 2019, Proximus received from Telenet a routine update of the data of the latter’s subscribers. That update contained new data for the complainant, which were not indicated as being confidential. That information was processed automatically by Proximus and was recorded, with the result that it was again included in the latter’s directories.  
26      On 14 August 2019, having realised that his telephone number had been published in the directories of Proximus and of third parties, the subscriber concerned again asked Proximus not to include his data in the directories. On the same date, Proximus replied to the complainant that it had withdrawn his data from the directories and contacted Google to have the relevant links to Proximus’ website deleted. Proximus also informed that subscriber that it had forwarded his contact details to other providers of directories and that, via the monthly updates, those providers had been informed of the complainant’s request.  
27      At the same time, the subscriber concerned submitted a complaint to the DPA against Proximus on the ground that, despite his request for his contact details not to be included in the directories, his telephone number was nevertheless included in some of those directories.  
28      On 5 September 2019, the complainant and Proximus had further exchanges concerning the publication of that subscriber’s data in the directory of a third party. In that context, Proximus stated that it forwards the contact details of its subscribers to other providers of directories, but that it is not in any way privy to the internal procedures of those providers.  
29      On 30 July 2020, after hearing both parties, the Geschillenkamer (Litigation Chamber) adopted a decision by which it ordered Proximus to take remedial action and to pay a fine of EUR 20 000 for infringement, inter alia, of Article 6 of the GDPR, read in conjunction with Article 7 thereof, and of Article 5(2) of that regulation, read in conjunction with Article 24 thereof. In particular, it first ordered Proximus to respond appropriately and immediately to the withdrawal of consent by the subscriber concerned and to comply with the requests of that subscriber seeking to exercise his right to erasure of the data concerning him. It then ordered Proximus to take appropriate technical and organisational measures to ensure that the processing of personal data that it performs complies with the provisions of the GDPR. Lastly, it ordered Proximus to cease unlawfully passing on the data concerned to other providers of directories.  
30      On 28 August 2020, Proximus brought an action against that decision before the hof van beroep te Brussel (Court of Appeal, Brussels).  
31      In Proximus’ view, in accordance with Article 45(3) of the Law on electronic communication, the consent of the subscriber is not required, rather subscribers must themselves request not to be included in the directories under an ‘opt-out’ system. In the absence of such a request, the subscriber concerned may in fact be included in those directories. Accordingly, in Proximus’ view, no ‘consent’ within the meaning of Directive 95/46 or within the meaning of the GDPR is, in the present case, required from the subscriber.  
32      Taking the opposite view, the DPA contended, in essence, that Article 12(2) of Directive 2002/58 and Article 133(1) of the Law on electronic communication require the ‘consent of subscribers’, within the meaning of the GDPR, in order for the providers of directories to be able to process and pass on their personal data.  
33      The referring court considers that Directive 2002/58 constitutes a   
lex specialis  
 in relation to the GDPR, as is confirmed by recital 173 and Article 95 of the GDPR. Consequently, in the situations in which Directive 2002/58 further specifies the GDPR rules, the specific provisions of that directive prevail as   
lex specialis  
 over the more general provisions of the GDPR.  
34      In that context, the referring court observes that Article 12(2) of Directive 2002/58 and Article 133(1) of the Law on electronic communication, while requiring an expression of the subscribers’ wishes in order for the providers of directories to be able to process their personal data, do not specify whether that expression of wishes must take the form of the exercise of a right of option, as Proximus maintains, or of the indication of genuine consent within the meaning of the GDPR, as stated by the DPA. On that point, the referring court notes that the Court’s case-law, in particular the judgment of 5 May 2011,   
Deutsche Telekom  
 (C-543/09, EU:C:2011:279, paragraph 61), established that – as follows from a contextual and systematic interpretation of Article 12 of Directive 2002/58 – the expression of wishes at issue corresponds to ‘consent’ in relation to the purpose of the publication of personal data in a public directory and not to the identity of any particular directory provider.  
35      Furthermore, given that no specific rules have been drawn up concerning the withdrawal by a subscriber of that expression of wishes or of that ‘consent’, neither in Directive 2002/58, nor in the Law on electronic communication, nor in an implementing decree, the referring court asks whether all the provisions of the GDPR must apply automatically and without any restrictions also in the particular context of telephone directories.  
36      In those circumstances the hof van beroep te Brussel (Court of Appeal, Brussels) decided to stay the proceedings and refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must Article 12(2) of [Directive 2002/58], read in conjunction with Article 2(f) thereof and Article 95 of the [GDPR] be interpreted as permitting a national supervisory authority to require a subscriber’s “consent” within the meaning of the [GDPR] as the basis for the publication of the subscriber’s personal data in public directories and directory enquiry services, published both by the operator itself and by third-party providers, in the absence of national legislation to the contrary?  
(2)      Must the right to erasure contained in Article 17 of the [GDPR] be interpreted as precluding a national supervisory authority from categorising a request by a subscriber to be removed from public directories and directory enquiry services as a request for erasure within the meaning of Article 17 of the [GDPR]?  
(3)      Must Article 24 and Article 5(2) of the [GDPR] be interpreted as precluding a national supervisory authority from concluding from the obligation of accountability laid down therein that the controller must take appropriate technical and organisational measures to inform third-party controllers, namely, the telephone service provider and other providers of directories and directory enquiry services which have received data from that first controller, of the withdrawal of the data subject’s consent in accordance with Article 6 in conjunction with Article 7 of the [GDPR]?  
(4)      Must Article 17(2) of the [GDPR] be interpreted as precluding a national supervisory authority from ordering a provider of public directories and directory enquiry services which has been requested to cease disclosing data relating to an individual to take reasonable steps to inform search engines of that request for erasure?’  
   
The questions referred for a preliminary ruling  
   
The first question  
37      Proximus submits that the case in the main proceedings does not concern the publication by a telephone service operator of directories containing personal data, with the result that the first question referred for a preliminary ruling should be considered inadmissible in so far as it concerns such a situation.  
38      In accordance with settled case-law, questions on the interpretation of EU law referred by a national court in the factual and legislative context which that court is responsible for defining, and the accuracy of which is not a matter for the Court to determine, enjoy a presumption of relevance. The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 48 and the case-law cited).  
39      In the present case, the dispute in the main proceedings is solely between a natural person and a company which is not his telephone service operator, regarding the manner in which that company processed the personal data of that person in the context of the publication of directories. It follows that the first question is inadmissible in so far as it seeks an interpretation of the requirements arising from Article 12(2) of Directive 2002/58 for the situation in which it is the telephone service operator of the person concerned that itself publishes his or her personal data in directories.  
40      It follows from the foregoing that, by its first question, the referring court asks, in essence, whether Article 12(2) of Directive 2002/58, read in conjunction with point (f) of the second paragraph of Article 2 of that directive and with Article 95 of the GDPR, must be interpreted as meaning that ‘consent’ within the meaning of Article 4(11) of the GDPR is required from the subscriber of a telephone service operator in order for that subscriber’s personal data to be included in directories published by providers other than that operator.  
41      In order to answer that question, it should be borne in mind that Article 1(1) of Directive 2002/58 provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with regard to the processing of personal data in the electronic communications sector.  
42      In that regard, it should be borne in mind that it is clear from Article 12(1) and recital 38 of that directive that, before being included in public directories, subscribers are to be informed of the purposes of the directory and of any particular usage which may be made of it, in particular through search functions embedded in the software of the electronic versions of the directories.  
43      Recital 39 of Directive 2002/58 further states, with respect to the obligation of prior information for subscribers under Article 12(1) thereof: ‘where the [personal] data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients’.  
44      After obtaining the information referred to in Article 12(1) of Directive 2002/58, the subscriber may – as is clear from Article 12(2) thereof – decide whether his or her personal data are to be included in a public directory and, if so, which personal data.  
45      As the Court has already held, such prior information gives the subscriber concerned the opportunity to give consent to the publication of his or her personal data in public directories, such consent being necessary for the purposes of such a publication (see, to that effect, judgment of 5 May 2011,   
Deutsche Telekom  
, C-543/09, EU:C:2011:279, paragraphs 54 and 58).  
46      The requirement to obtain the consent of the subscriber concerned for the purposes of publishing those data in directories is confirmed in Article 12(3) of Directive 2002/58, according to which Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name, ‘additional consent be asked of the subscribers’.  
47      However, as the Court has stated, it follows from a contextual and systematic interpretation of Article 12 of Directive 2002/58 that the consent under Article 12(2) relates to the purpose of the publication of personal data in a public directory and not to the identity of any particular directory provider. Accordingly, where the subscriber concerned has consented to his or her data being published in a directory with a specific purpose, he or she will generally not have standing to object to the publication of the same data in another, similar directory (judgment of 5 May 2011,   
Deutsche Telekom  
, C-543/09, EU:C:2011:279, paragraphs 61 and 62).  
48      In that regard, recital 39 of Directive 2002/58 confirms that the passing of subscribers’ personal data to third parties is ‘subject to the condition that the data may not be used for other purposes than those for which they were collected’.  
49      It follows that where a subscriber has been informed by a telephone service operator, such as Telenet, of the possibility that his or her personal data may be passed to a third-party undertaking, such as Proximus or other third parties, with a view to being published in a public directory, and where that subscriber has consented to the publication of those data in such a directory, renewed consent is not needed from the subscriber concerned for the passing of those same data by that operator or by that undertaking to another undertaking which intends to publish a printed or electronic public directory, or to make such directories available for consultation through directory enquiry services, if it is guaranteed that the data in question will not be used for purposes other than those for which the data were collected with a view to their first publication. The consent given under Article 12(2) of Directive 2002/58, by a subscriber who has been duly informed, to the publication of his or her personal data in a public directory relates to the purpose of that publication and thus extends to any subsequent processing of those data by third-party undertakings active in the market for publicly available directory enquiry services and directories, provided that such processing pursues that same purpose (judgment of 5 May 2011,   
Deutsche Telekom  
, C-543/09, EU:C:2011:279, paragraph 65).  
50      However, as stated in recital 39 of that directive, if the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.  
51      As regards the manner in which such consent must be indicated, it follows from point (f) of the second paragraph of Article 2 of Directive 2002/58, read in conjunction with Article 94(2) and Article 95 of the GDPR, that such consent must, in principle, meet the requirements under Article 4(11) of that regulation.  
52      In the present case, Article 4(11) of the GDPR, which constitutes the provision applicable to the facts at issue in the main proceedings, defines the ‘consent of the data subject’ as requiring a ‘freely given, specific, informed and unambiguous’ indication of the data subject’s wishes in the form of a statement or of ‘a clear affirmative action’ signifying agreement to the processing of personal data relating to him or her.  
53      It follows that such consent is necessary in order for the personal data relating to the subscriber of a telephone service operator to be included in directories.  
54      Consequently, the publication of the personal data relating to the subscriber in question in directories such as those published by Proximus or by other providers can be regarded as lawful within the meaning of Article 6(1)(a) of the GDPR only if such consent exists, having been expressly given to the telephone service operator or to one of those providers of directories.  
55      However, as has been noted in paragraph 49 above, such consent does not presuppose that, on the date on which it is given, the data subject is necessarily aware of the identity of all the providers of directories which will process his or her personal data.  
56      In the light of the foregoing considerations, the answer to the first question is that Article 12(2) of Directive 2002/58, read in conjunction with point (f) of the second paragraph of Article 2 thereof and with Article 95 of the GDPR, must be interpreted as meaning that ‘consent’ within the meaning of Article 4(11) of the GDPR is required from the subscriber of a telephone service operator in order for the personal data of that subscriber to be included in directories published by providers other than that operator, and that that consent may be provided to that operator or to one of those providers.  
   
The second question  
57      By its second question, the referring court asks, in essence, whether Article 17 of the GDPR must be interpreted as meaning that the request by a subscriber to have his or her personal data withdrawn from directories constitutes making use of the ‘right to erasure’ within the meaning of that article.  
58      It should first of all be noted that Proximus submits that Article 17 of the GDPR is not applicable to a provider of directories which, as in the present case, is not the subscriber’s telephone service operator and that a request, such as that referred to in the preceding paragraph, should, at most, have to be regarded as constituting a request for rectification within the meaning of Article 16 of that regulation. Accordingly, the second question referred for a preliminary ruling is inadmissible in that it is irrelevant to the case in the main proceedings.  
59      However, the arguments put forward by that party relate, in essence, to the field of application and scope, and therefore to the interpretation, of the provisions of EU law to which the second question relates. Such arguments, which concern the substance of the question referred, cannot therefore, by their very nature, lead to the inadmissibility of the question (judgment of 13 January 2022,   
Minister Sprawiedliwości  
, C-55/20, EU:C:2022:6, paragraph 83).  
60      It follows that the second question referred for a preliminary ruling is admissible.  
61      In the first place, it should be noted that, under the second sentence of Article 12(2) of Directive 2002/58, subscribers must have, inter alia, the opportunity to have the personal data relating to them withdrawn from public directories.  
62      However, the grant of such an opportunity to subscribers does not constitute, as regards the providers of directories, a specific obligation, within the meaning of Article 95 of the GDPR, which would make it possible to exclude the application of the relevant provisions of that regulation. As the Advocate General observed, in essence, in point 54 of his Opinion, Directive 2002/58 does not contain any indications as to the modalities, implementation and consequences of requests to obtain the withdrawal of personal data. Accordingly, as is apparent, moreover, from recital 10 of that directive, read in conjunction with Article 94 of the GDPR, the provisions of the GDPR may be applied in such a situation.  
63      In the second place, it follows from Article 17(1)(b) and (d) of the GDPR that the data subject is to have the right to obtain from the controller the erasure of personal data concerning him or her and that the controller is to have the obligation to erase those data without undue delay, inter alia where the data subject ‘withdraws consent on which the processing is based according to point (a) of Article 6(1) … and where there is no other legal ground for the processing’ or even where ‘the personal data have been unlawfully processed’.  
64      In that regard, first, it follows from the answer to the first question referred for a preliminary ruling that the publication of a subscriber’s personal data in directories is based on that subscriber’s consent.  
65      Secondly, it is apparent from Article 6(1)(a) and Article 7(3) of the GDPR that such consent constitutes one of the necessary conditions for a finding that the processing of the personal data of the subscriber concerned is lawful, and that that consent may be withdrawn at any time and in a manner which is as easy as that which enabled the data subject to give such consent.  
66      In the present case, when the subscriber requests that his or her data no longer be included in a directory, he or she is withdrawing his or her consent to the publication of those data. On the basis of the withdrawal of his or her consent, he or she obtains, in the absence of another legal ground for such processing, the right to request the erasure of his or her personal data from that directory pursuant to Article 17(1)(b) of the GDPR or, where the controller continues to publish those data unlawfully, pursuant to Article 17(1)(d) of that regulation.  
67      In those circumstances, it must be concluded that the request by a subscriber to have his or her personal data withdrawn from directories may be regarded as making use of the ‘right to erasure’ of those data within the meaning of Article 17 of the GDPR.  
68      That conclusion cannot be called into question by Proximus’ argument that such a request should be regarded as seeking to allow that subscriber to exercise his or her right to obtain from the controller the rectification of the personal data concerning him or her, pursuant to Article 16 of the GDPR. Under that provision, such a rectification is possible where those data are inaccurate and is intended to allow the data subject to have those data completed.  
69      However, in the present case, a request for withdrawal of a subscriber’s data contained in a directory does not seek to replace inaccurate data with correct data or to complete incomplete data, but to withdraw the publication of correct data.  
70      The fact that such a withdrawal takes the form, in the present case, of the mere adjustment of the code assigned to the subscriber concerned in Proximus’ database – from which that subscriber’s personal data are published in the directories – cannot prevent a request for withdrawal of personal data contained in those directories from being regarded as a ‘request for erasure’ within the meaning of Article 17 of the GDPR. As is apparent from the documents before the Court, the method of withdrawal provided for by the operator in question constitutes a purely technical or organisational measure which proves necessary to respond to the request for erasure of the data subject’s personal data and to prevent the disclosure of those data.  
71      In the light of the foregoing considerations, the answer to the second question is that Article 17 of the GDPR must be interpreted as meaning that the request by a subscriber to have his or her personal data withdrawn from directories constitutes making use of the ‘right to erasure’ within the meaning of that article.  
   
The third question  
72      By its third question, the referring court asks, in essence, whether Article 5(2) and Article 24 of the GDPR must be interpreted as meaning that a national supervisory authority may require that a provider of directories, as controller, take appropriate technical and organisational measures to inform third-party controllers, namely the telephone service operator which has communicated its subscriber’s personal data to that provider and the other providers of directories to which that provider has itself supplied such data, of the withdrawal of the subscriber’s consent.  
73      As a preliminary point, it should be noted that, in the present case, Proximus processed personal data of the complainant by publishing them and by communicating them to other providers of directories. Telenet, the complainant’s telephone service operator, also processed those data, inter alia by passing them on to Proximus. The same is true of the other providers of directories that received the complainant’s contact details from Proximus and that published them.  
74      In addition, it should be noted, first, that, as has been pointed out in paragraph 20 above, although the Law on electronic communication requires telephone service operators to pass on the data relating to their subscribers to providers of public directories, those operators must, however, keep separate the data relating to subscribers who have indicated that they do not wish to be included in a directory so as to allow those subscribers to receive a copy of that directory without their data being included therein.  
75      It is apparent from the documents before the Court that, in practice, it is usually to his or her telephone service operator that the subscriber gives his or her consent to the publication of his or her personal data in a directory, such consent making it possible for those data to be transferred to a third-party provider of directories. That provider may, in turn, communicate such data to other providers of directories on the basis of the same consent, those controllers thus constituting a chain in which each in turn processes the data in question independently on the basis of one and the same consent.  
76      Secondly, it is also apparent from the documents before the Court that the update of Proximus’ database, which was intended to give effect to the withdrawal of the complainant’s consent, was erased as soon as the complainant’s telephone service operator sent Proximus a new list of data relating to its subscribers – for the purposes of publication of those data in the directories – which did not take into account the fact that the complainant had notified Proximus of the withdrawal of his consent.  
77      In that context, the question thus arises whether a provider of directories such as Proximus, when a subscriber of a telephone service operator withdraws his or her consent to be included in the directories of that provider, must not only update its own database to take account of that withdrawal, but must also notify the withdrawal both to the telephone service operator which has communicated the data concerned to that provider and also to the other providers of directories to which that provider has itself forwarded such data.  
78      In the first place, it should be recalled that Article 6(1)(a) of the GDPR provides that processing is to be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes. However, it is apparent from the order for reference that the complainant withdrew his consent, within the meaning of Article 7(3) of that regulation, to the processing of his personal data for the purposes of their publication in directories. Following such a withdrawal, the processing of those data for the purposes of their inclusion in public directories, including that performed for the same purpose by the telephone service operators or by other providers of directories on the basis of the same consent, no longer has any legal ground and is thus unlawful in the light of Article 6(1)(a) of the GDPR.  
79      In the second place, it should be recalled that, in accordance with Article 5(1)(a) and (2) of the GDPR, the controller must ensure that it is able to demonstrate that personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject.  
80      As regards Article 24 of the GDPR, that provision requires that, taking into account the nature, scope, context and purposes of processing, the controller implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with that regulation.  
81      As the Advocate General observed in point 67 of his Opinion, Article 5(2) and Article 24 of the GDPR impose general accountability and compliance requirements upon controllers of personal data. In particular, those provisions require controllers to take appropriate steps to prevent any infringements of the rules laid down in the GDPR in order to ensure the right to the protection of data.  
82      From that point of view, Article 19 of the GDPR provides, inter alia, that the controller is to communicate any erasure of personal data carried out in accordance with Article 17(1) of that regulation to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.  
83      It follows from the general obligations laid down in Article 5(2) and Article 24 of the GDPR, read in conjunction with Article 19 thereof, that a controller of personal data, such as Proximus, must, by means of appropriate technical and organisational measures, inform the other providers of directories that have received such data from it of the withdrawal of the data subject’s consent addressed to it. In circumstances such as those set out in paragraph 76 above, such a controller must also ensure that the telephone service operator that has communicated those personal data to it is informed so that that operator amends the list of personal data that it automatically forwards to that provider of directories and keeps separate the data of its subscribers who have indicated their wish to withdraw their consent to those data being made public.  
84      Where, as in the present case, various controllers rely on the single consent of the data subject in order to process his or her personal data for the same purpose, it is sufficient, in order for that data subject to withdraw such consent, that he or she contacts, for the purposes of the withdrawal requested, any one of the controllers which rely on that same consent.  
85      As the Commission correctly observes, in order to ensure the effectiveness of the right of the data subject to withdraw his or her consent provided for in Article 7(3) of the GDPR and to ensure that the data subject’s consent is strictly linked to the purpose for which it was given, the controller to which the data subject has notified the withdrawal of his or her consent to the processing of his or her personal data is in fact required to communicate that withdrawal to any person who has forwarded those data to it and to the person to whom it has, in turn, forwarded those data. The controllers thus informed are then, in turn, obliged to forward that information to the other controllers to which they have communicated such data.  
86      In that regard, it should, first of all, be noted that such an information obligation is intended to prevent any possible infringement of the rules laid down in the GDPR in order to ensure the right to the protection of data and thus forms part of the appropriate measures within the meaning of Article 24 of that regulation. Furthermore, as the Advocate General stated in point 68 of his Opinion, it also forms part of the requirement laid down in Article 12(2) of the GDPR, pursuant to which the controller must facilitate the exercise of the rights conferred on the data subject, inter alia, by Article 17 of that regulation.  
87      Next, it must be found that the absence of such an obligation on the controller to communicate the withdrawal of the data subject’s consent could make the withdrawal of consent particularly difficult, since that data subject might consider himself or herself required to contact each of the operators. Such an approach would thus be contrary to Article 7(3) of the GDPR, which provides that it must be as easy to withdraw, as to give, consent to the processing of personal data.  
88      Lastly, in accordance with the case-law referred to in paragraph 49 above, the consent given under Article 12(2) of Directive 2002/58, by a subscriber who has been duly informed, to the publication of his or her personal data in a public directory relates to the purpose of that publication and thus extends to any subsequent processing of those data by third-party undertakings active in the market for directories, provided that such processing pursues that same purpose.  
89      It follows that, as the Advocate General observed in point 68 of his Opinion, since a provider of directories may rely on the consent given by a subscriber, to the processing of data for that same purpose, to another provider or to his or her telephone service operator, it must be possible for a subscriber, in order to withdraw consent, to contact any one of the providers of directories or that telephone service operator with a view to his or her contact details being withdrawn from directories published by all of those who rely upon his or her single expression of consent.  
90      In the light of the foregoing considerations, the answer to the third question is that Article 5(2) and Article 24 of the GDPR must be interpreted as meaning that a national supervisory authority may require that the provider of directories, as controller, take appropriate technical and organisational measures to inform third-party controllers, namely the telephone service operator which has communicated its subscriber’s personal data to that provider and the other providers of directories to which that provider has itself supplied such data, of the withdrawal of the subscriber’s consent.  
   
The fourth question  
91      By its fourth question, the referring court asks, in essence, whether Article 17(2) of the GDPR must be interpreted as precluding a national supervisory authority from ordering a provider of directories – which has been requested by the subscriber of a telephone service operator to cease disclosing personal data relating to him or her – to take ‘reasonable steps’, within the meaning of that provision, to inform search engine providers of that request for erasure of the data.  
92      In order to answer that question, it should be borne in mind that Article 17(2) of the GDPR imposes the obligation on the controller which has made the personal data public, taking account of available technology and the cost of implementation, to take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.  
93      As is apparent from recital 66 of the GDPR, the objective of that obligation is to strengthen the right to be forgotten in the online environment, and therefore specifically applies to information made available on the internet by search engine providers that process data published online.  
94      In the present case, it is common ground that Proximus published, in its directory, the complainant’s personal data and, therefore, that that company must be regarded as a controller which has made such data public within the meaning of Article 17(2) of the GDPR.  
95      Furthermore, it must be borne in mind, first, that, in accordance with settled case-law, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing’ of personal data within the meaning of Article 4(2) of the GDPR when that information contains personal data and, second, that the operator of that search engine must be regarded as the ‘controller’ in respect of that processing, within the meaning of Article 4(7), and therefore also of Article 17(2), of that regulation (see, to that effect, judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 35 and the case-law cited).  
96      Accordingly, in circumstances such as those at issue in the main proceedings, it must be concluded that a controller such as Proximus is required, under Article 17(2) of the GDPR, to ensure that reasonable steps are taken to inform search engine providers of the request addressed to it by the subscriber of a telephone service operator for erasure of his or her personal data. However, as the Advocate General observed in point 76 of his Opinion, in order to assess the reasonableness of the steps taken by the provider of directories, Article 17(2) of the GDPR provides that the available technology and the cost of implementation must be taken into account, a task that falls primarily upon the authority competent for such matters, subject to judicial review.  
97      In the present case, it is apparent from the written observations lodged by the DPA, which have not been challenged on that point by the other parties to the present proceedings, that, during the second quarter of 2020, there were a limited number of search engine providers operating in Belgium. In particular, Google had a market share of between 90%, as regards desktop searches, and 99%, as regards smartphone and tablet searches.  
98      In addition, as stated in paragraph 26 above, it is apparent from the documents before the Court that, in response to the subscriber’s request for his data not to be included in the directories of that provider, Proximus stated that it had not only withdrawn those data from the telephone directories and from the directory enquiry services, but that it had also contacted Google to have the relevant links to Proximus’ website deleted.  
99      In the light of the foregoing considerations, the answer to the fourth question is that Article 17(2) of the GDPR must be interpreted as not precluding a national supervisory authority from ordering a provider of directories – which has been requested by the subscriber of a telephone service operator to cease disclosing personal data relating to him or her – to take ‘reasonable steps’, within the meaning of that provision, to inform search engine providers of that request for erasure of the data.  
   
Costs  
100    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Fourth Chamber) hereby rules:  
1.        
Article 12(2) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in conjunction with point (f) of the second paragraph of Article 2 of that directive and with Article 95 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),  
must be interpreted as meaning that ‘consent’ within the meaning of Article 4(11) of that regulation is required from the subscriber of a telephone service operator in order for the personal data of that subscriber to be included in publicly available telephone directories and directory enquiry services published by providers other than that operator, and that that consent may be provided to that operator or to one of those providers.  
2.        
Article 17 of Regulation 2016/679  
must be interpreted as meaning that the request by a subscriber to have his or her personal data withdrawn from publicly available telephone directories and directory enquiry services constitutes making use of the ‘right to erasure’ within the meaning of that article.  
3.        
Article 5(2) and Article 24 of Regulation 2016/679  
must be interpreted as meaning that a national supervisory authority may require that the provider of publicly available telephone directories and directory enquiry services, as controller, take appropriate technical and organisational measures to inform third-party controllers, namely the telephone service operator that has communicated its subscriber’s personal data to that provider and the other providers of publicly available telephone directories and directory enquiry services to which that provider has itself supplied such data, of the withdrawal of the subscriber’s consent.  
4.        
Article 17(2) of Regulation 2016/679  
must be interpreted as not precluding a national supervisory authority from ordering a provider of publicly available telephone directories and directory enquiry services – which has been requested by the subscriber of a telephone service operator to cease disclosing personal data relating to him or her – to take ‘reasonable steps’, within the meaning of that provision, to inform search engine providers of that request for erasure of the data.

ID: bde96cde-7301-4304-bc4c-32ecb77aee48

of 9 Feb 2023, C-453/21 (  
X-FAB Dresden  
)  
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Data protection officer   
   
JUDGMENT OF THE COURT (Sixth Chamber)  
9 February 2023 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 38(3) – Data protection officer – Prohibition on dismissing data protection officer for performing his or her tasks – Requirement for functional independence – National legislation prohibiting the dismissal of a data protection officer without just cause – Article 38(6) – Conflict of interests – Criteria)  
In Case C-453/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesarbeitsgericht (Federal Labour Court, Germany), made by decision of 27 April 2021, received at the Court on 21 July 2021, in the proceedings  
X-FAB Dresden GmbH & Co. KG  
v  
FC,  
THE COURT (Sixth Chamber),  
composed of P.G. Xuereb, President of the Chamber, A. Kumin and I. Ziemele (Rapporteur), Judges,  
Advocate General: J. Richard de la Tour,  
Registrar: D. Dittert, head of unit,  
having regard to the written procedure and further to the hearing on 26 September 2022,  
after considering the observations submitted on behalf of:  
–        X-FAB Dresden GmbH & Co. KG, by S. Leese, Rechtsanwalt,  
–        FC, by R. Buschmann and T. Heller, Prozessbevollmächtigte,  
–        the German Government, by J. Möller, D. Klebs and P.-L. Krüger, acting as Agents,  
–        the European Parliament, by O. Hrstková Šolcová and B. Schäfer, acting as Agents,  
–        the Council of the European Union, by T. Haas and K. Pleśniak, acting as Agents,  
–        the European Commission, by A. Bouchagiar, K. Herrmann and H. Kranenborg, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation and validity of the second sentence of Article 38(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2; ‘the GDPR’) and the interpretation of Article 38(6) of that regulation.  
2        The request has been made in proceedings between X-FAB Dresden GmbH & Co. KG (‘X-FAB’) and FC, an employee of X-FAB, concerning FC’s dismissal from the position of data protection officer (the ‘DPO’), carried out by X-FAB.  
   
Legal context  
   
European Union law  
3        Recitals 10 and 97 of the GDPR state:  
‘(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
…  
(97)      … Such [DPOs], whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.’  
4        Article 37 of the GDPR, entitled ‘Designation of the [DPO]’, provides in paragraphs 5 and 6:  
‘5.      The [DPO] shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.  
6.      The [DPO] may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.’  
5        Article 38 of the GDPR, entitled ‘Position of the [DPO]’, provides in paragraphs 3, 5 and 6:  
‘3.      The controller and processor shall ensure that the [DPO] does not receive any instructions regarding the exercise of those tasks. [The DPO] shall not be dismissed or penalised by the controller or the processor for performing his tasks. The [DPO] shall directly report to the highest management level of the controller or processor.  
…  
5.      The [DPO] shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.  
6.      The [DPO] may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.’  
6        Article 39 of the GDPR, entitled ‘Tasks of the [DPO]’, reads as follows:  
‘1.      The [DPO] shall have at least the following tasks:  
(a)      to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;  
(b)      to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;  
(c)      to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;  
(d)      to cooperate with the supervisory authority;  
(e)      to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.  
2.      The [DPO] shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.’  
   
German law  
   
The BDSG  
7        Paragraph 6 of the Bundesdatenschutzgesetz (Federal Law on data protection) of 20 December 1990 (BGBl. 1990 I, p. 2954), in the version in force from 25 May 2018 until 25 November 2019 (BGBl. 2017 I, p. 2097) (‘the BDSG’), entitled ‘Position’, provides in subparagraph 4:  
‘The dismissal of the [DPO] shall be permitted only by applying Paragraph 626 of the Bürgerliches Gesetzbuch (Civil Code) in the version of 2 January 2002 (BGBl. 2002 I, p. 42, corrigenda BGBl. 2002 I, p. 2909, and BGBl. 2003 I, p. 738) accordingly. The [DPO]’s employment shall not be terminated unless there are facts that give the public body just cause to terminate without notice. The [DPO]’s employment shall not be terminated for one year after the activity as the data protection officer has ended, unless the public body has just cause to terminate without notice.’  
8        Paragraph 38 of the BDSG, entitled ‘[DPO] of private bodies’, states:  
‘(1)      In addition to Article 37(1)(b) and (c) of the [GDPR], the controller and processor shall designate a [DPO] if they generally continuously employ at least ten persons dealing with the automated processing of personal data. …  
(2)      Paragraph 6(4), (5) second sentence, and (6) shall apply; however, Paragraph 6(4) shall apply only if the designation of a data protection officer is mandatory.’  
   
The Civil Code  
9        Paragraph 626 of the Civil Code, entitled ‘Termination without notice with just cause’, provides:  
‘(1)      The employment relationship may be terminated by either party to the contract with just cause without giving notice where facts are present on the basis of which the terminating party cannot reasonably be expected to continue the employment relationship to the end of the notice period or to the agreed end of the employment relationship, taking all circumstances of the individual case into account and weighing the interests of both parties to the contract.  
(2)      Termination may take place only upon expiry of a period of two weeks. That period starts to run when the person entitled to terminate becomes aware of the facts serving as the basis for termination. …’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
10      FC is employed by X-FAB as from 1 November 1993.  
11      He performs the duties of chair of the works council in that company and, on that basis, is released from some of his work obligations. He also holds the role of vice-chair of the central works council which was established for three undertakings in the group of companies to which X-FAB belongs, which are established in Germany.  
12      With effect from 1 June 2015, FC was appointed, by each undertaking separately, as the DPO of X-FAB, its parent company and the other subsidiaries of the parent company established in Germany. According to the referring court, the aim of that appointment in parallel of FC as the DPO of all those undertakings was to ensure a uniform level of data protection in those undertakings.  
13      At the request of the state officer for data protection and freedom of information of Thüringen (Germany), X-FAB and the undertakings referred to in paragraph 12 of the present judgment, by letters dated 1 December 2017, dismissed FC with immediate effect from his duties as DPO. By separate letters of 25 May 2018, those undertakings, as a precautionary measure, repeated their dismissal of FC, based on the second sentence of Article 38(3) of the GDPR, which had in the intervening period become applicable, relying on grounds linked to the group of companies to which X-FAB belongs.  
14      The action brought by FC before the German courts seeks a declaration that he retains the position of DPO of X-FAB. X-FAB submits that there is a risk of a conflict of interests if FC simultaneously performs the functions of DPO and chair of the works council, on the ground that those two posts are incompatible. There is, therefore, a just cause justifying FC’s dismissal as DPO.  
15      The courts of first instance and of appeal upheld FC’s action. The appeal on a point of law (  
Revision  
) brought by X-FAB before the Bundesarbeitsgericht (Federal Labour Court, Germany), which is the referring court, seeks to have that action dismissed.  
16      The referring court observes that the outcome of that appeal depends on the interpretation of EU law. In particular, the question arises, first, whether the second sentence of Article 38(3) of the GDPR precludes the legislation of a Member State from making the dismissal of a DPO subject to stricter conditions than those laid down by EU law and, if so, whether that provision has sufficient legal basis. Should the Court find that the conditions to which the BDSG makes the dismissal subject do comply with EU law, it would be necessary to determine whether the functions of chair of the works council and of DPO of that undertaking may be performed by one and the same person or whether that would give rise to a conflict of interests within the meaning of the second sentence of Article 38(6) of the GDPR.  
17      In those circumstances the Bundesarbeitsgericht (Federal Labour Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is the second sentence of Article 38(3) of [the GDPR] to be interpreted as precluding a provision in national law, such as, in the present case, Paragraph 38(1) and (2) in conjunction with the first sentence of Paragraph 6(4) of the [BDSG], which makes dismissal of the [DPO] by the controller, who is his employer, subject to certain conditions set out therein, irrespective of whether such dismissal relates to the performance of his tasks?  
If the first question is answered in the affirmative:  
(2)      Does the second sentence of Article 38(3) GDPR also preclude such a provision in national law if the designation of the [DPO] is mandatory not in accordance with Article 37(1) GDPR, but only in accordance with the law of the Member State?  
If the first question is answered in the affirmative:  
(3)      Does the second sentence of Article 38(3) of the GDPR have sufficient legal basis, in particular in so far as it covers [DPOs] that have an employment relationship with the controller?  
If the first question is answered in the negative:  
(4)      Is there a conflict of interests within the meaning of the second sentence of Article 38(6) of the GDPR if the [DPO] also holds the office of [chair] of the works council established at the controlling body? Must specific tasks have been assigned within the works council in order for such a conflict of interests to be assumed to exist?’  
   
Consideration of the questions referred  
   
The first question  
18      By its first question, the referring court asks, in essence, whether the second sentence of Article 38(3) of the GDPR must be interpreted as precluding national legislation which provides that a controller or a processor may dismiss a DPO who is a member of staff of that controller or processor solely where there is just cause, even if the dismissal is not related to the performance of that officer’s tasks.  
19      As is clear from settled case-law, in interpreting a provision of EU law, it is necessary to consider not only its wording, by considering the latter’s usual meaning in everyday language, but also the context in which the provision occurs and the objectives pursued by the rules of which it is part (judgment of 22 June 2022,  
 Leistritz  
, C-534/20, EU:C:2022:495, paragraph 18 and the case-law cited).  
20      In the first place, as regards the wording of the provision at issue, it must be stated that the second sentence of Article 38(3) of the GDPR provides that ‘he or she shall not be dismissed or penalised by the controller or the processor for performing his [or her] tasks’.  
21      In that regard, in its judgment of 22 June 2022,  
 Leistritz  
 (C-534/20, EU:C:2022:495, paragraphs 20 and 21), the Court, after observing that the GDPR does not define the terms ‘dismissed’, ‘penalised’ and ‘for performing his [or her] tasks’ in the second sentence of Article 38(3) of the GDPR, stated, first, that, in accordance with the meaning which those words have in everyday language, the prohibition of the dismissal, by a controller or processor, of a DPO or of the imposition, by a controller or processor, of a penalty on him or her means that that DPO must be protected against any decision terminating his or her duties, by which he or she would be placed at a disadvantage or which would constitute a penalty.  
22      A dismissal measure in respect of a DPO taken by his or her employer and resulting in the DPO being dismissed by the controller or its processor is capable of constituting such a decision.  
23      Second, as the Court has also stated, the second sentence of Article 38(3) of the GDPR applies without distinction both to the DPO who is a member of the staff of the controller or processor and to the person who fulfils the tasks on the basis of a service contract concluded with the latter, in accordance with Article 37(6) of the GDPR, with the result that the second sentence of Article 38(3) is intended to apply to relationships between a DPO and a controller or processor, irrespective of the nature of the relationship between that DPO and the latter (judgment of 22 June 2022,  
 Leistritz  
, C-534/20, EU:C:2022:495, paragraphs 23 and 24).  
24      Third, the latter provision imposes a limit which consists in prohibiting the dismissal of a DPO on a ground relating to the performance of his or her tasks, which include, in particular, under Article 39(1)(b) of the GDPR, monitoring compliance with EU or Member State legal provisions on data protection and with the policies of the controller or processor concerning the protection of personal data (see, to that effect, judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 25).  
25      In the second place, as regards the objective pursued by the second sentence of Article 38(3) of the GDPR, first, recital 97 of that regulation states that data protection officers, whether or not they are employees of the controller, should be in a position to perform their duties and tasks in an independent manner. In that regard, such independence must necessarily enable them to carry out those tasks in accordance with the objective of the GDPR, which seeks, inter alia, as is apparent from recital 10 thereof, to ensure a high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union (judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 26 and the case-law cited).  
26      Second, the objective of ensuring the functional independence of the DPO, as it follows from the second sentence of Article 38(3) of the GDPR, is also apparent from the first and third sentences of that provision, which require that that DPO is not to receive any instructions regarding the exercise of those tasks and is to report directly to the highest level of management of the controller or processor, and from Article 38(5), which provides that, with regard to that exercise, that DPO is to be bound by secrecy or confidentiality (judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 27).  
27      Thus, the second sentence of Article 38(3) of the GDPR, by protecting the DPO against any decision which terminates his or her duties, places him or her at a disadvantage or constitutes a penalty, where such a decision relates to the performance of his or her tasks, must be regarded as seeking essentially to preserve the functional independence of the DPO and, therefore, to ensure that the provisions of the GDPR are effective (judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 28).  
28      As the Court has also held, that interpretation is supported, in the third place, by the context of that provision and, in particular, by the legal basis on which the EU legislature adopted the GDPR (judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 29).  
29      As is apparent from the preamble to the GDPR, that regulation was adopted on the basis of Article 16 TFEU, paragraph 2 of which provides, in particular, that the European Parliament and the Council of the European Union are, by means of regulations, acting in accordance with the ordinary legislative procedure, to lay down the rules relating, first, to the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices or agencies and by the Member States when carrying out activities which fall within the scope of EU law and, second, to the free movement of such data (judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 30).  
30      In that regard, the laying down of rules on protection against the dismissal of a DPO employed by a controller or by a processor falls within the scope of the protection of natural persons with regard to the processing of personal data solely inasmuch as such rules are intended to preserve the functional independence of the latter, in accordance with the second sentence of Article 38(3) of the GDPR (see, to that effect, judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 31).  
31      It follows that each Member State is free, in the exercise of its retained competence, to lay down more protective specific provisions on the dismissal of the DPO, in so far as those provisions are compatible with EU law and, in particular, with the provisions of the GDPR, particularly the second sentence of Article 38(3) thereof (see, to that effect, judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 34).  
32      In particular, such increased protection cannot undermine the achievement of the objectives of the GDPR. That would be the case if it prevented any dismissal, by a controller or by a processor, of a DPO who no longer possesses the professional qualities required to perform his or her tasks, in accordance with Article 37(5) of the GDPR, or who does not fulfil those tasks in accordance with the provisions of that regulation (see, to that effect, judgment of 22 June 2022,   
Leistritz  
, C-534/20, EU:C:2022:495, paragraph 35).  
33      In that regard, it should be recalled, as has been noted in paragraph 25 of the present judgment, that the GDPR seeks to ensure a high level of protection of natural persons within the European Union with regard to the processing of their personal data, and that, in order to achieve that objective, the DPO must be in a position to perform his or her duties and tasks in an independent manner.  
34      Thus, increased protection for the DPO which would prevent the dismissal of the DPO in the event that he or she is not, or is no longer, in a position to carry out his or her tasks in an independent manner on account of there being a conflict of interests would undermine the achievement of that objective.  
35      It is for the national court to satisfy itself that specific provisions such as those referred to in paragraph 31 of the present judgment are compatible with EU law and, in particular, with the provisions of the GDPR.  
36      In the light of the foregoing considerations, the answer to the first question is that the second sentence of Article 38(3) of the GDPR must be interpreted as not precluding national legislation which provides that a controller or a processor may dismiss a DPO who is a member of staff of that controller or processor solely where there is just cause, even if the dismissal is not related to the performance of that DPO’s tasks, in so far as such legislation does not undermine the achievement of the objectives of the GDPR.  
   
The second and third questions  
37      In the light of the answer given to the first question, there is no need to answer the second and third questions.  
   
The fourth question  
38      By its fourth question, the referring court asks, in essence, in which circumstances may the existence of a ‘conflict of interests’, within the meaning of Article 38(6) of the GDPR, be established.  
39      As regards, in the first place, the wording of the provision at issue, it should be noted that, as set out in the second sentence of Article 38(6) of the GDPR, ‘the [DPO] may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests’.  
40      It thus follows from the wording of that provision, first, that the GDPR does not establish that there is a fundamental incompatibility between, on the one hand, the performance of DPO’s duties and, on the other hand, the performance of other duties within the controller or processor. Article 38(6) of that regulation specifically provides that the DPO may be entrusted with performing tasks and duties other than those for which it is responsible under Article 39 of the GDPR.  
41      The fact remains, second, that the controller or its processor must ensure that those other tasks and duties do not give rise to a ‘conflict of interests’. In the light of the meaning of those words in everyday language, it must be held that, in accordance with the objective pursued by Article 38(6) of the GDPR, the DPO cannot be entrusted with performing tasks or duties which could impair the execution of the functions performed by the DPO.  
42      As regards that objective, it should, in the second place, be noted that that provision is, in essence, intended, as are the other provisions referred to in paragraph 25 of the present judgment, to preserve the functional independence of the DPO and, consequently, to ensure the effectiveness of the provisions of the GDPR.  
43      In the third place, as regards the context of which Article 38(6) of the GDPR forms part, it should be noted that, according to Article 39(1)(b) of the GDPR, the task of the DPO is, inter alia, to monitor compliance with the GDPR, other provisions of EU law or of the law of the Member States on data protection and the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.  
44      It follows, in particular, that a DPO cannot be entrusted with tasks or duties which would result in him or her determining the objectives and methods of processing personal data on the part of the controller or its processor. Under EU law or the law of the Member States on data protection, the review of those objectives and methods must be carried out independently by the DPO.  
45      The determination of the existence of a conflict of interests, within the meaning of Article 38(6) of the GDPR, must be carried out, case by case, on the basis of an assessment of all the relevant circumstances, in particular the organisational structure of the controller or its processor and in the light of all the applicable rules, including any policies of the controller or its processor.  
46      In the light of all the foregoing, the answer to the fourth question is that Article 38(6) of the GDPR must be interpreted as meaning that a ‘conflict of interests’, as provided for in that provision, may exist where a DPO is entrusted with other tasks or duties, which would result in him or her determining the objectives and methods of processing personal data on the part of the controller or its processor, which is a matter for the national court to determine, case by case, on the basis of an assessment of all the relevant circumstances, in particular the organisational structure of the controller or its processor and in the light of all the applicable rules, including any policies of the controller or its processor.  
   
Costs  
47      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Sixth Chamber) hereby rules:  
1.        
The second sentence of Article 38(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as not precluding national legislation which provides that a controller or a processor may dismiss a data protection officer who is a member of staff of that controller or processor solely where there is just cause, even if the dismissal is not related to the performance of that officer’s tasks, in so far as such legislation does not undermine the achievement of the objectives of that regulation.  
2.        
Article 38(6) of Regulation 2016/679 must be interpreted as meaning that a ‘conflict of interests’, as provided for in that provision, may exist where a data protection officer is entrusted with other tasks or duties, which would result in him or her determining the objectives and methods of processing personal data on the part of the controller or its processor, which is a matter for the national court to determine, case by case, on the basis of an assessment of all the relevant circumstances, in particular the organisational structure of the controller or its processor and in the light of all the applicable rules, including any policies of the controller or its processor.

ID: becee8e7-196b-41b2-b60c-164334f97ac3

Judgment of 6 Nov 2003, C-101/01 (  
Bodil Lindqvist  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Processing   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Household exemption   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Special categories of personal data   
General data protection law   
 >   
Chapter V - International data transfer   
 >   
General principle for transfers   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - General   
   
JUDGMENT OF THE COURT  
6 November 2003 (1)  
(Directive 95/46/EC - Scope - Publication of personal data on the internet - Place of publication - Definition of transfer of personal data to third countries - Freedom of expression - Compatibility with Directive 95/46 of greater protection for personal data under the national legislation of a Member State)  
In Case C-101/01,  
REFERENCE to the Court under Article 234 EC by the Göta hovrätt (Sweden) for a preliminary ruling in the criminal proceedings before that court against  
 Bodil Lindqvist,  
on, inter alia, the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31),  
THE COURT,  
composed of: P. Jann, President of the First Chamber, acting for the President, C.W.A. Timmermans, C. Gulmann, J.N. Cunha Rodrigues and A. Rosas (Presidents of Chambers), D.A.O. Edward (Rapporteur), J.-P. Puissochet, F. Macken and S. von Bahr, Judges,  
Advocate General: A. Tizzano,  
Registrar: H. von Holstein, Deputy Registrar,  
after considering the written observations submitted on behalf of:  
-    Mrs Lindqvist, by S. Larsson, advokat,   
-    the Swedish Government, by A. Kruse, acting as Agent,   
-    the Netherlands Government, by H.G. Sevenster, acting as Agent,   
-    the United Kingdom Government, by G. Amodeo, acting as Agent, assisted by J. Stratford, barrister,   
-    the Commission of the European Communities, by L. Ström and X. Lewis, acting as Agents,   
having regard to the Report for the Hearing,  
after hearing the oral observations of Mrs Lindqvist, represented by S. Larsson, of the Swedish Government, represented by A. Kruse and B. Hernqvist, acting as Agents, of the Netherlands Government, represented by J. van Bakel, acting as Agent, of the United Kingdom Government, represented by J. Stratford, of the Commission, represented by L. Ström and C. Docksey, acting as Agent, and of the EFTA Surveillance Authority, represented by D. Sif Tynes, acting as Agent, at the hearing on 30 April 2002,  
after hearing the Opinion of the Advocate General at the sitting on 19 September 2002,  
gives the following  
Judgment  
1.     By order of 23 February 2001, received at the Court on 1 March 2001, the Göta hovrätt (Göta Court of Appeal) referred to the Court for a preliminary ruling under Article 234 EC seven questions concerning inter alia the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).   
2.     Those questions were raised in criminal proceedings before that court against Mrs Lindqvist, who was charged with breach of the Swedish legislation on the protection of personal data for publishing on her internet site personal data on a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church.   
 Legal background  
Community legislation  
3.     Directive 95/46 is intended, according to the terms of Article 1(1), to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.   
4.     Article 3 of Directive 95/46 provides, regarding the scope of the directive:   
1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.  
2. This Directive shall not apply to the processing of personal data:  
-    in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,   
-    by a natural person in the course of a purely personal or household activity.   
5.     Article 8 of Directive 95/46, entitled The processing of special categories of data, provides:   
1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.  
2. Paragraph 1 shall not apply where:  
(a)    the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or   
(b)    processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards; or   
(c)    processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or   
(d)    processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or   
(e)    the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.   
3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.  
4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.  
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.  
Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.  
6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.  
7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.  
6.     Article 9 of Directive 95/46, entitled Processing of personal data and freedom of expression, provides:   
Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.  
7.     Article 13 of Directive 95/46, entitled Exemptions and restrictions, provides that Member States may adopt measures restricting the scope of some of the obligations imposed by the directive on the controller of the data, inter alia as regards information given to the persons concerned, where such a restriction is necessary to safeguard, for example, national security, defence, public security, an important economic or financial interest of a Member State or of the European Union, or the investigation and prosecution of criminal offences or of breaches of ethics for regulated professions.   
8.     Article 25 of Directive 95/46, which is part of Chapter IV entitled Transfer of personal data to third countries, reads as follows:       
   
1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.  
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.  
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.  
4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.  
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.  
6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.  
Member States shall take the measures necessary to comply with the Commission's decision.  
9.     At the time of the adoption of Directive 95/46, the Kingdom of Sweden made the following statement on the subject of Article 9, which was entered in the Council minutes (document No 4649/95 of the Council, of 2 February 1995):   
The Kingdom of Sweden considers that artistic and literary expression refers to the means of expression rather than to the contents of the communication or its quality.  
 10.     The European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950 (the ECHR), provides, in Article 8, for a right to respect for private and family life and, in Article 10, contains provisions concerning freedom of expression.   
The national legislation  
11.     Directive 95/46 was implemented in Swedish law by the Personuppgiftslag (SFS 1998:204) (Swedish law on personal data, the PUL).   
 The main proceedings and the questions referred  
12.     In addition to her job as a maintenance worker, Mrs Lindqvist worked as a catechist in the parish of Alseda (Sweden). She followed a data processing course on which she had inter alia to set up a home page on the internet. At the end of 1998, Mrs Lindqvist set up internet pages at home on her personal computer in order to allow parishioners preparing for their confirmation to obtain information they might need. At her request, the administrator of the Swedish Church's website set up a link between those pages and that site.   
13.     The pages in question contained information about Mrs Lindqvist and 18 colleagues in the parish, sometimes including their full names and in other cases only their first names. Mrs Lindqvist also described, in a mildly humorous manner, the jobs held by her colleagues and their hobbies. In many cases family circumstances and telephone numbers and other matters were mentioned. She also stated that one colleague had injured her foot and was on half-time on medical grounds.   
14.     Mrs Lindqvist had not informed her colleagues of the existence of those pages or obtained their consent, nor did she notify the Datainspektionen (supervisory authority for the protection of electronically transmitted data) of her activity. She removed the pages in question as soon as she became aware that they were not appreciated by some of her colleagues.   
15.     The public prosecutor brought a prosecution against Mrs Lindqvist charging her with breach of the PUL on the grounds that she had:   
-    processed personal data by automatic means without giving prior written notification to the Datainspektionen (Paragraph 36 of the PUL);   
-    processed sensitive personal data (injured foot and half-time on medical grounds) without authorisation (Paragraph 13 of the PUL);   
-    transferred processed personal data to a third country without authorisation (Paragraph 33 of the PUL).   
   
16.     Mrs Lindqvist accepted the facts but disputed that she was guilty of an offence. Mrs Lindqvist was fined by the Eksjö tingsrätt (District Court) (Sweden) and appealed against that sentence to the referring court.   
17.     The amount of the fine was SEK 4 000, which was arrived at by multiplying the sum of SEK 100, representing Mrs Lindqvist's financial position, by a factor of 40, reflecting the severity of the offence. Mrs Lindqvist was also sentenced to pay SEK 300 to a Swedish fund to assist victims of crimes.   
18.     As it had doubts as to the interpretation of the Community law applicable in this area, inter alia Directive 95/46, the Göta hovrätt decided to stay proceedings and refer the following questions to the Court for a preliminary ruling:   
(1)    Is the mention of a person - by name or with name and telephone number - on an internet home page an action which falls within the scope of [Directive 95/46]? Does it constitute the processing of personal data wholly or partly by automatic means to list on a self-made internet home page a number of persons with comments and statements about their jobs and hobbies etc.?   
(2)    If the answer to the first question is no, can the act of setting up on an internet home page separate pages for about 15 people with links between the pages which make it possible to search by first name be considered to constitute the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system within the meaning of Article 3(1)?   
If the answer to either of those questions is yes, the hovrätt also asks the following questions:  
(3)    Can the act of loading information of the type described about work colleagues onto a private home page which is none the less accessible to anyone who knows its address be regarded as outside the scope of [Directive 95/46] on the ground that it is covered by one of the exceptions in Article 3(2)?   
(4)    Is information on a home page stating that a named colleague has injured her foot and is on half-time on medical grounds personal data concerning health which, according to Article 8(1), may not be processed?   
(5)    [Directive 95/46] prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden - with the result that personal data become accessible to people in third countries - does that constitute a transfer of data to a third country within the meaning of the directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?   
(6)    Can the provisions of [Directive 95/46], in a case such as the above, be regarded as bringing about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the EU and are enshrined in inter alia Article 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms?   
Finally, the hovrätt asks the following question:  
(7)    Can a Member State, as regards the issues raised in the above questions, provide more extensive protection for personal data or give it a wider scope than the directive, even if none of the circumstances described in Article 13 exists?   
 The first question  
19.     By its first question, the referring court asks whether the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46.   
Observations submitted to the Court  
20.     Mrs Lindqvist submits that it is unreasonable to take the view that the mere mention by name of a person or of personal data in a document contained on an internet page constitutes automatic processing of data. On the other hand, reference to such data in a keyword in the meta tags of an internet page, which makes it possible to create an index and find that page using a search engine, might constitute such processing.   
21.     The Swedish Government submits that the term the processing of personal data wholly or partly by automatic means in Article 3(1) of Directive 95/46, covers all processing in computer format, in other words, in binary format. Consequently, as soon as personal data are processed by computer, whether using a word processing programme or in order to put them on an internet page, they have been the subject of processing within the meaning of Directive 95/46.   
22.     The Netherlands Government submits that personal data are loaded onto an internet page using a computer and a server, which are essential elements of automation, so that it must be considered that such data are subject to automatic processing.   
23.     The Commission submits that Directive 95/46 applies to all processing of personal data referred to in Article 3 thereof, regardless of the technical means used. Accordingly, making personal data available on the internet constitutes processing wholly or partly by automatic means, provided that there are no technical limitations which restrict the processing to a purely manual operation. Thus, by its very nature, an internet page falls within the scope of Directive 95/46.   
Reply of the Court  
24.     The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies.   
25.     According to the definition in Article 2(b) of Directive 95/46, the term processing of such data used in Article 3(1) covers any operation or set of operations which is performed upon personal data, whether or not by automatic means. That provision gives several examples of such operations, including disclosure by transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing.   
26.     It remains to be determined whether such processing is wholly or partly by automatic means. In that connection, placing information on an internet page entails, under current technical and computer procedures, the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet. Such operations are performed, at least in part, automatically.   
27.     The answer to the first question must therefore be that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46.   
 The second question  
28.     As the first question has been answered in the affirmative, there is no need to reply to the second question, which arises only in the event that the first question is answered in the negative.   
   
 The third question  
29.     By its third question, the national court essentially seeks to know whether processing of personal data such as that described in the first question is covered by one of the exceptions in Article 3(2) of Directive 95/46.   
Observations submitted to the Court  
30.     Mrs Lindqvist submits that private individuals who make use of their freedom of expression to create internet pages in the course of a non-profit-making or leisure activity are not carrying out an economic activity and are thus not subject to Community law. If the Court were to hold otherwise, the question of the validity of Directive 95/46 would arise, as, in adopting it, the Community legislature would have exceeded the powers conferred on it by Article 100a of the EC Treaty (now, after amendment, Article 95 EC). The approximation of laws, which concerns the establishment and functioning of the common market, cannot serve as a legal basis for Community measures regulating the right of private individuals to freedom of expression on the internet.   
31.     The Swedish Government submits that, when Directive 95/46 was implemented in national law, the Swedish legislature took the view that processing of personal data by a natural person which consisted in publishing those data to an indeterminate number of people, for example through the internet, could not be described as a purely personal or household activity within the meaning of the second indent of Article 3(2) of Directive 95/46. However, that Government does not rule out that the exception provided for in the first indent of that paragraph might cover cases in which a natural person publishes personal data on an internet page solely in the exercise of his freedom of expression and without any connection with a professional or commercial activity.   
32.     According to the Netherlands Government, automatic processing of data such as that at issue in the main proceedings does not fall within any of the exceptions in Article 3(2) of Directive 95/46. As regards the exception in the second indent of that paragraph in particular, it observes that the creator of an internet page brings the data placed on it to the knowledge of a generally indeterminate group of people.   
33.     The Commission submits that an internet page such as that at issue in the main proceedings cannot be considered to fall outside the scope of Directive 95/46 by virtue of Article 3(2) thereof, but constitutes, given the purpose of the internet page at issue in the main proceedings, an artistic and literary creation within the meaning of Article 9 of that Directive.   
 34.     It takes the view that the first indent of Article 3(2) of Directive 95/46 lends itself to two different interpretations. The first consists in limiting the scope of that provision to the areas cited as examples, in other words, to activities which essentially fall within what are generally called the second and third pillars. The other interpretation consists in excluding from the scope of Directive 95/46 the exercise of any activity which is not covered by Community law.   
35.     The Commission argues that Community law is not limited to economic activities connected with the four fundamental freedoms. Referring to the legal basis of Directive 95/46, to its objective, to Article 6 EU, to the Charter of fundamental rights of the European Union proclaimed in Nice on 18 December 2000 (OJ 2000 C 364, p. 1), and to the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, it concludes that that directive is intended to regulate the free movement of personal data in the exercise not only of an economic activity, but also of social activity in the course of the integration and functioning of the common market.   
36.     It adds that to exclude generally from the scope of Directive 95/46 internet pages which contain no element of commerce or of provision of services might entail serious problems of demarcation. A large number of internet pages containing personal data intended to disparage certain persons with a particular end in view might then be excluded from the scope of that directive.   
Reply of the Court  
37.     Article 3(2) of Directive 95/46 provides for two exceptions to its scope.   
38.     The first exception concerns the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.   
39.     As the activities of Mrs Lindqvist which are at issue in the main proceedings are essentially not economic but charitable and religious, it is necessary to consider whether they constitute the processing of personal data in the course of an activity which falls outside the scope of Community law within the meaning of the first indent of Article 3(2) of Directive 95/46.   
40.     The Court has held, on the subject of Directive 95/46, which is based on Article 100a of the Treaty, that recourse to that legal basis does not presuppose the existence of an actual link with free movement between Member States in every situation referred to by the measure founded on that basis (see Joined Cases C-465/00, C-138/01 and C-139/01   
Österreichischer Rundfunk and Others  
 [2003] ECR I-4989, paragraph 41, and the case-law cited therein).   
   
41.     A contrary interpretation could make the limits of the field of application of the directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations (  
Österreichischer Rundfunk and Others  
, cited above, paragraph 42).   
42.     Against that background, it would not be appropriate to interpret the expression activity which falls outside the scope of Community law as having a scope which would require it to be determined in each individual case whether the specific activity at issue directly affected freedom of movement between Member States.   
43.     The activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 (in other words, the activities provided for by Titles V and VI of the Treaty on European Union and processing operations concerning public security, defence, State security and activities in areas of criminal law) are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals.   
44.     It must therefore be considered that the activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 are intended to define the scope of the exception provided for there, with the result that that exception applies only to the activities which are expressly listed there or which can be classified in the same category (  
ejusdem generis  
).   
45.     Charitable or religious activities such as those carried out by Mrs Lindqvist cannot be considered equivalent to the activities listed in the first indent of Article 3(2) of Directive 95/46 and are thus not covered by that exception.   
46.     As regards the exception provided for in the second indent of Article 3(2) of Directive 95/46, the 12th recital in the preamble to that directive, which concerns that exception, cites, as examples of the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses.   
47.     That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.   
48.     The answer to the third question must therefore be that processing of personal data such as that described in the reply to the first question is not covered by any of the exceptions in Article 3(2) of Directive 95/46.   
   
 The fourth question  
49.     By its fourth question, the referring court seeks to know whether reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.   
50.     In the light of the purpose of the directive, the expression data concerning health used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual.   
51.     The answer to the fourth question must therefore be that reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.   
 The fifth question  
52.     By its fifth question the referring court seeks essentially to know whether there is any transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person (the hosting provider) who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country. The referring court also asks whether the reply to that question would be the same if no one from the third country had in fact accessed the data or if the server where the page was stored was physically in a third country.   
Observations submitted to the Court  
53.     The Commission and the Swedish Government consider that the loading, using a computer, of personal data onto an internet page, so that they become accessible to nationals of third countries, constitutes a transfer of data to third countries within the meaning of Directive 95/46. The answer would be the same if no one from the third country had in fact accessed the data or if the server where it was stored was physically in a third country.   
54.     The Netherlands Government points out that the term transfer is not defined by Directive 95/46. It takes the view, first, that that term must be understood to refer to the act of intentionally transferring personal data from the territory of a Member State to a third country and, second, that no distinction can be made between the different ways in which data are made accessible to third parties. It concludes that loading personal data onto an internet page using a computer cannot be considered to be a transfer of personal data to a third country within the meaning of Article 25 of Directive 95/46.   
55.     The United Kingdom Government submits that Article 25 of Directive 95/46 concerns the transfer of data to third countries and not their accessibility from third countries. The term transfer connotes the transmission of personal data from one place and person to another place and person. It is only in the event of such a transfer that Article 25 of Directive 95/46 requires Member States to ensure an adequate level of protection of personal data in a third country.   
Reply of the Court  
56.     Directive 95/46 does not define the expression transfer to a third country in Article 25 or any other provision, including Article 2.   
57.     In order to determine whether loading personal data onto an internet page constitutes a transfer of those data to a third country within the meaning of Article 25 of Directive 95/46 merely because it makes them accessible to people in a third country, it is necessary to take account both of the technical nature of the operations thus carried out and of the purpose and structure of Chapter IV of that directive where Article 25 appears.   
58.     Information on the internet can be consulted by an indefinite number of people living in many places at almost any time. The ubiquitous nature of that information is a result inter alia of the fact that the technical means used in connection with the internet are relatively simple and becoming less and less expensive.   
59.     Under the procedures for use of the internet available to individuals like Mrs Lindqvist during the 1990s, the author of a page intended for publication on the internet transmits the data making up that page to his hosting provider. That provider manages the computer infrastructure needed to store those data and connect the server hosting the site to the internet. That allows the subsequent transmission of those data to anyone who connects to the internet and seeks access to it. The computers which constitute that infrastructure may be located, and indeed often are located, in one or more countries other than that where the hosting provider is established, without its clients being aware or being in a position to be aware of it.   
60.     It appears from the court file that, in order to obtain the information appearing on the internet pages on which Mrs Lindqvist had included information about her colleagues, an internet user would not only have to connect to the internet but also personally carry out the necessary actions to consult those pages. In other words, Mrs Lindqvist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages.   
   
61.     It follows that, in circumstances such as those in the case in the main proceedings, personal data which appear on the computer of a person in a third country, coming from a person who has loaded them onto an internet site, were not directly transferred between those two people but through the computer infrastructure of the hosting provider where the page is stored.   
62.     It is in that light that it must be examined whether the Community legislature intended, for the purposes of the application of Chapter IV of Directive 95/46, to include within the expression transfer [of data] to a third country within the meaning of Article 25 of that directive activities such as those carried out by Mrs Lindqvist. It must be stressed that the fifth question asked by the referring court concerns only those activities and not those carried out by the hosting providers.   
63.     Chapter IV of Directive 95/46, in which Article 25 appears, sets up a special regime, with specific rules, intended to allow the Member States to monitor transfers of personal data to third countries. That Chapter sets up a complementary regime to the general regime set up by Chapter II of that directive concerning the lawfulness of processing of personal data.   
64.     The objective of Chapter IV is defined in the 56th to 60th recitals in the preamble to Directive 95/46, which state inter alia that, although the protection of individuals guaranteed in the Community by that Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection, the adequacy of such protection must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations. Where a third country does not ensure an adequate level of protection the transfer of personal data to that country must be prohibited.   
65.     For its part, Article 25 of Directive 95/46 imposes a series of obligations on Member States and on the Commission for the purposes of monitoring transfers of personal data to third countries in the light of the level of protection afforded to such data in each of those countries.   
66.     In particular, Article 25(4) of Directive 95/46 provides that, where the Commission finds that a third country does not ensure an adequate level of protection, Member States are to take the measures necessary to prevent any transfer of personal data to the third country in question.   
67.     Chapter IV of Directive 95/46 contains no provision concerning use of the internet. In particular, it does not lay down criteria for deciding whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located.   
68.     Given, first, the state of development of the internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.   
69.     If Article 25 of Directive 95/46 were interpreted to mean that there is transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.   
70.     Accordingly, it must be concluded that Article 25 of Directive 95/46 is to be interpreted as meaning that operations such as those carried out by Mrs Lindqvist do not as such constitute a transfer [of data] to a third country. It is thus unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country.   
71.     The reply to the fifth question must therefore be that there is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.   
 The sixth question  
72.     By its sixth question the referring court seeks to know whether the provisions of Directive 95/46, in a case such as that in the main proceedings, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined in inter alia Article 10 of the ECHR.   
Observations submitted to the Court  
73.     Citing inter alia Case C-274/99 P   
Connolly  
 v   
Commission  
 [2001] ECR I-1611, Mrs Lindqvist submits that Directive 95/46 and the PUL, in so far as they lay down requirements of prior consent and prior notification of a supervisory authority and a principle of prohibiting processing of personal data of a sensitive nature, are contrary to the general principle of freedom of expression enshrined in Community law. More particularly, she argues that the definition of processing of personal data wholly or partly by automatic means does not fulfil the criteria of predictability and accuracy.   
74.     She argues further that merely mentioning a natural person by name, revealing their telephone details and working conditions and giving information about their state of health and hobbies, information which is in the public domain, well-known or trivial, does not constitute a significant breach of the right to respect for private life. Mrs Lindqvist considers that, in any event, the constraints imposed by Directive 95/46 are disproportionate to the objective of protecting the reputation and private life of others.   
75.     The Swedish Government considers that Directive 95/46 allows the interests at stake to be weighed against each other and freedom of expression and protection of private life to be thereby safeguarded. It adds that only the national court can assess, in the light of the facts of each individual case, whether the restriction on the exercise of the right to freedom of expression entailed by the application of the rules on the protection of the rights of others is proportionate.   
76.     The Netherlands Government points out that both freedom of expression and the right to respect for private life are among the general principles of law for which the Court ensures respect and that the ECHR does not establish any hierarchy between the various fundamental rights. It therefore considers that the national court must endeavour to balance the various fundamental rights at issue by taking account of the circumstances of the individual case.   
77.     The United Kingdom Government points out that its proposed reply to the fifth question, set out in paragraph 55 of this judgment, is wholly in accordance with fundamental rights and avoids any disproportionate restriction on freedom of expression. It adds that it is difficult to justify an interpretation which would mean that the publication of personal data in a particular form, that is to say, on an internet page, is subject to far greater restrictions than those applicable to publication in other forms, such as on paper.   
78.     The Commission also submits that Directive 95/46 does not entail any restriction contrary to the general principle of freedom of expression or other rights and freedoms applicable in the European Union corresponding inter alia to the right provided for in Article 10 of the ECHR.   
Reply of the Court  
79.     According to the seventh recital in the preamble to Directive 95/46, the establishment and functioning of the common market are liable to be seriously affected by differences in national rules applicable to the processing of personal data. According to the third recital of that directive the harmonisation of those national rules must seek to ensure not only the free flow of such data between Member States but also the safeguarding of the fundamental rights of individuals. Those objectives may of course be inconsistent with one another.   
80.     On the one hand, the economic and social integration resulting from the establishment and functioning of the internal market will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States, whether businesses or public authorities of the Member States. Those so involved will, to a certain extent, need to have access to personal data to perform their transactions or carry out their tasks within the area without internal frontiers which the internal market constitutes.   
81.     On the other hand, those affected by the processing of personal data understandably require those data to be effectively protected.   
82.     The mechanisms allowing those different rights and interests to be balanced are contained, first, in Directive 95/46 itself, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for. Second, they result from the adoption, by the Member States, of national provisions implementing that directive and their application by the national authorities.   
83.     As regards Directive 95/46 itself, its provisions are necessarily relatively general since it has to be applied to a large number of very different situations. Contrary to Mrs Lindqvist's contentions, the directive quite properly includes rules with a degree of flexibility and, in many instances, leaves to the Member States the task of deciding the details or choosing between options.   
84.     It is true that, in many respects, the Member States have a margin for manoeuvre in implementing Directive 95/46. However, there is nothing to suggest that the regime it provides for lacks predictability or that its provisions are, as such, contrary to the general principles of Community law and, in particular, to the fundamental rights protected by the Community legal order.   
85.     Thus, it is, rather, at the stage of the application at national level of the legislation implementing Directive 95/46 in individual cases that a balance must be found between the rights and interests involved.   
86.     In that context, fundamental rights have a particular importance, as demonstrated by the case in the main proceedings, in which, in essence, Mrs Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site.   
   
87.     Consequently, it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality.   
88.     Whilst it is true that the protection of private life requires the application of effective sanctions against people processing personal data in ways inconsistent with Directive 95/46, such sanctions must always respect the principle of proportionality. That is so   
a fortiori  
 since the scope of Directive 95/46 is very wide and the obligations of those who process personal data are many and significant.   
89.     It is for the referring court to take account, in accordance with the principle of proportionality, of all the circumstances of the case before it, in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed.   
90.     The answer to the sixth question must therefore be that the provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the ECHR. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order.   
 The seventh question  
91.     By its seventh question, the referring court essentially seeks to know whether it is permissible for the Member States to provide for greater protection for personal data or a wider scope than are required under Directive 95/46.   
Observations submitted to the Court  
92.     The Swedish Government states that Directive 95/46 is not confined to fixing minimum conditions for the protection of personal data. Member States are obliged, in the course of implementing that directive, to attain the level of protection dictated by it and are not empowered to provide for greater or less protection. However, account must be taken of the discretion which the Member States have in implementing the directive to lay down in their domestic law the general conditions for the lawfulness of the processing of personal data.   
93.     The Netherlands Government submits that Directive 95/46 does not preclude Member States from providing for greater protection in certain areas. It is clear, for example, from Article 10, Article 11(1), subparagraph (a) of the first paragraph of Article 14, Article 17(3), Article 18(5) and Article 19(1) of that directive that the Member States may make provision for wider protection. Moreover, the Member States are free to apply the principles of Directive 95/46 also to activities which do not fall within its scope.   
94.     The Commission submits that Directive 95/46 is based on Article 100a of the Treaty and that, if a Member State wishes to maintain or introduce legislation which derogates from such a harmonising directive, it is obliged to notify the Commission pursuant to Article 95(4) or 95(5) EC. The Commission therefore submits that a Member State cannot make provision for more extensive protection for personal data or a wider scope than are required under the directive.   
Reply of the Court  
95.     Directive 95/46 is intended, as appears from the eighth recital in the preamble thereto, to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. The tenth recital adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.   
96.     The harmonisation of those national laws is therefore not limited to minimal harmonisation but amounts to harmonisation which is generally complete. It is upon that view that Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate.   
97.     It is true that Directive 95/46 allows the Member States a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations as a large number of its provisions demonstrate. However, such possibilities must be made use of in the manner provided for by Directive 95/46 and in accordance with its objective of maintaining a balance between the free movement of personal data and the protection of private life.   
98.     On the other hand, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof, provided that no other provision of Community law precludes it.   
99.     In the light of those considerations, the answer to the seventh question must be that measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it.   
 Costs  
100.     The costs incurred by the Swedish, Netherlands and United Kingdom Governments and by the Commission and the EFTA Surveillance Authority, which have submitted observations to the Court, are not recoverable. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court.   
On those grounds,  
THE COURT,  
in answer to the questions referred to it by the Göta hovrätt by order of 23 February 2001, hereby rules:  
 1.    The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.   
2.    Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46.   
3.    Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.   
4.    There is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.   
 5.    The provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order.   
6.    Measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it.   
JannTimmermans Gulmann   
Cunha RodriguesRosas Edward   
Puissochet Macken von Bahr   
Delivered in open court in Luxembourg on 6 November 2003.  
R. Grass V. Skouris   
RegistrarPresident   
1: Language of the case: Swedish.   
  
  
  
  
Disclaimer

ID: c359ff09-64a4-44f8-ab1a-3cefd08c9cc3

of 11 Apr 2024, C-741/21 (  
juris  
)  
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Right to compensation and liability   
   
JUDGMENT OF THE COURT (Third Chamber)  
11 April 2024 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 82 – Right to compensation for damage caused by data processing that infringes that regulation – Concept of ‘non-material damage’ – Impact of the seriousness of the damage suffered – Liability of the controller – Possible exemption in the event of default of a person acting under his or her authority within the meaning of Article 29 – Assessment of the amount of compensation – Inapplicability of the criteria laid down for administrative fines in Article 83 – Assessment in the event of multiple infringements of that regulation)  
In Case C-741/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Landgericht Saarbrücken (Regional Court, Saarbrücken, Germany), made by decision of 22 November 2021, received at the Court on 1 December 2021, in the proceedings  
GP  
v  
juris GmbH,  
THE COURT (Third Chamber),  
composed of K. Jürimäe, President of the Chamber, N. Piçarra and N. Jääskinen (Rapporteur), Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        GP, by H. Schöning, Rechtsanwalt,  
–        juris GmbH, by E. Brandt and C. Werkmeister, Rechtsanwälte,  
–        Ireland, by M. Browne, Chief State Solicitor, A. Joyce and M. Lane, acting as Agents, and by D. Fennelly, Barrister-at-Law,  
–        the European Commission, by A. Bouchagiar, M. Heller and H. Kranenborg, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 82(1) and (3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’), read in conjunction with Articles 29 and 83 of that regulation and in the light of recitals 85 and 146 thereof.  
2        The request has been made in proceedings between GP, a natural person, and juris GmbH, a company established in Germany, concerning compensation for the damage that GP claims to have suffered as a result of various processing operations involving his personal data which were carried out for marketing purposes, despite the objections he had sent to that company.  
   
Legal context  
3        Recitals 85, 146 and 148 of the GDPR are worded as follows:  
‘(85)      A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. …  
…  
(146)      The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. … Data subjects should receive full and effective compensation for the damage they have suffered. …  
…  
(148)      In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation … . Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. …’  
4        Article 4 of that regulation, entitled ‘Definitions’, provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); …  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …  
…  
(12)      “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;  
…’  
5        Article 5 of that regulation sets out a series of principles relating to the processing of personal data.  
6        Article 21 of the GDPR, entitled “Right to object”, which is contained in Chapter III of the GDPR relating to “Rights of the data subject”, provides, in paragraph 3:  
‘Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.’  
7        Chapter IV of that regulation, entitled ‘Controller and processor’, contains Articles 24 to 43 thereof.  
8        Article 24 of that regulation, entitled ‘Responsibility of the controller’, states in paragraphs 1 and 2:  
‘1.      Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.  
2.      Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.’  
9        Article 25 of that regulation, entitled ‘Data protection by design and by default’ provides, in paragraph 1 thereof:  
Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.’  
10      Article 29 of the GDPR, entitled ‘Processing under the authority of the controller and processor’, provides:  
‘The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.’  
11      Article 32 of that regulation, entitled ‘Security of processing’, states:  
‘1.      Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:  
…  
(b)      the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;  
…  
2.      In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.  
…  
4.      The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.’  
12      Chapter VIII of the GDPR, entitled ‘Remedies, liability and penalties’, contains Articles 77 to 84 of that regulation.  
13      Article 79 of that regulation, entitled ‘Right to an effective judicial remedy against a controller or processor’, provides in paragraph 1 thereof:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’  
14      Article 82 of that regulation, entitled ‘Right to compensation and liability’, states in paragraphs 1 to 3:  
‘1.      Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.  
2.      Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. …  
3.      A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.’  
15      Article 83 of the GDPR, entitled ‘General conditions for imposing administrative fines’, states, in paragraphs 2, 3 and 5:  
‘2.      … When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:  
(a)      the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;  
(b)      the intentional or negligent character of the infringement;  
…  
(k)      any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.  
3.      If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.  
…  
5.      Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:  
(a)      the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;  
(b)      the data subjects’ rights pursuant to Articles 12 to 22;  
…’  
16      Article 84 of that regulation, entitled ‘Penalties’, provides, in paragraph 1 thereof:  
‘Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
17      The applicant in the main proceedings, a natural person practising as a self-employed lawyer, was a client of juris, a company operating a legal database.  
18      On 6 November 2018, after learning that his personal data were also being used by juris for the purposes of direct marketing, the applicant in the main proceedings revoked, in writing, all his consents to receive information from that company by email or by telephone, and he objected to any processing of those data, except for the purposes of sending newsletters which he wished to continue to receive.  
19      Despite that step, the applicant in the main proceedings received, in January 2019, two advertising leaflets sent by name to his business address. By email sent to juris on 18 April 2019, he reminded juris of his prior objection to any marketing, he informed juris that the creation of those prospectuses had given rise to unlawful processing of his data and requested compensation for the damage suffered by him under Article 82 of the GDPR. Upon receiving a new advertising leaflet on 3 May 2019, he reiterated his objection, which was this time served on juris by bailiff.  
20      Each of those leaflets contained a ‘trial personal code’ giving access, on the juris website, to an order form for that company’s products which included information relating to the applicant in the main proceedings, as was established, at the latter’s request, by a notary on 7 June 2019.  
21      The applicant in the main proceedings brought an action before the Landgericht Saarbrücken (Regional Court, Saarbrücken, Germany), which is the referring court in the present case, seeking, on the basis of Article 82(1) of the GDPR, compensation for his material damage, relating to the costs of the bailiff and notary incurred by him, and for his non-material damage. He submits, inter alia, that he has suffered a loss of control over his personal data as a result of the processing of those data by juris despite his objections, and that he is entitled to obtain compensation on that basis, without having to show the effects or gravity of the infringement of his rights, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union and specified in that regulation.  
22      In its defence, juris dismisses any liability, arguing that it had indeed established a system for managing objections to marketing and that the late taking into account of those of the applicant in the main proceedings was due either to the fact that one of its employees had not complied with the instructions given or to the fact that it would have been excessively onerous to take those objections into account. It claims that the mere breach of an obligation under the GDPR, such as that under Article 21(3) thereof, cannot, in itself, constitute ‘damage’ within the meaning of Article 82(1) of that regulation.  
23      In the first place, the referring court starts from the premiss that the right to compensation under Article 82(1) of the GDPR is subject to the fulfilment of three conditions, namely an infringement of that regulation, material or non-material damage, and a causal link between that infringement and that damage. Next, in view of the claims of the applicant in the main proceedings, the referring court asks whether it should nevertheless be held that an infringement of the GDPR constitutes, in itself, non-material damage giving rise to a right to compensation, in particular where the infringed provision of that regulation confers a subjective right on the data subject. Lastly, given that German law makes monetary compensation for non-material damage subject to the requirement of serious harm to the protected rights, that court asks whether a similar restriction must apply to claims for compensation under the GDPR, in the light of the guidance relating to the concept of ‘damage’ in recitals 85 and 146 of that regulation.  
24      In the second place, that court considers it possible that it follows from Article 82 of the GDPR that, where an infringement of that regulation has been established, that infringement is deemed to be attributable to the controller, with the result that there is liability for presumed fault, or even no fault, on the part of the controller. Furthermore, after pointing out that paragraph 3 of that article does not specify the evidential requirements specifically linked to the exemption provided for in that paragraph, the referring court observes that, if the controller were allowed to avoid liability by merely relying, in general terms, on wrongful conduct on the part of one of its employees, that would significantly limit the effectiveness of the right to compensation provided for in paragraph 1 of that article.  
25      In the third place, the referring court wishes to know, inter alia, whether, in order to assess the amount of monetary compensation for damage, in particular non-material damage, which would be due under Article 82 of the GDPR, the criteria laid down in Article 83(2) and (5) of that regulation for deciding the amount of administrative fines may, or indeed must, also be taken into account in the context of Article 82.  
26      In the fourth and final place, that court notes that, in the dispute before it, the personal data of the applicant in the main proceedings have been processed on several occasions for the purposes of marketing, despite the repeated objections of the data subject. It therefore seeks to determine whether, where there are such multiple infringements of the GDPR, those infringements must be taken into account individually or globally, with a view to setting the amount of compensation that may be due under Article 82 of that regulation.  
27      In those circumstances, the Landgericht Saarbrücken (Regional Court, Saarbrücken) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      In the light of recital 85 and the third sentence of recital 146 of the GDPR, is the concept of ‘non-material damage’ in Article 82(1) of the GDPR to be understood as covering any impairment of the protected legal position, irrespective of the other effects and materiality of that impairment?  
(2)      Is liability for compensation under Article 82(3) of the GDPR excluded by the fact that the infringement is attributed to human error in the individual case on the part of a person acting under the authority of the processor or controller within the meaning of Article 29 of the GDPR?  
(3)      Is it permissible or necessary [to base] the assessment of compensation for non-material damage [on the] criteria for determining fines set out in Article 83 of the GDPR, in particular in Article 83(2) and 83(5) of the GDPR?  
(4)      Must the compensation be determined for each individual infringement, or are several infringements – or at least several infringements of the same nature – penalised by means of an overall amount of compensation, which is not determined by adding up individual amounts but is based on an evaluative overall assessment?’  
   
Consideration of the questions referred  
   
The first question  
   
Admissibility  
28      As a preliminary point, juris submits, in essence, that the first question is inadmissible in so far as it seeks to establish whether entitlement to compensation under Article 82 of the GDPR is subject to the requirement that the damage alleged by the data subject, as defined in Article 4(1) of that regulation, has reached a certain degree of seriousness. That question is, it contends, irrelevant to the resolution of the dispute in the main proceedings, on the ground that the damage alleged by the applicant in the main proceedings, namely a loss of control over his personal data, did not occur, since those data were lawfully processed, as part of the contractual relationship between the parties to that dispute.  
29      In that connection, it must be borne in mind that it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court, which enjoy a presumption of relevance. Therefore, since the question referred concerns the interpretation or validity of a rule of EU law, the Court is, in principle, required to give a ruling, unless it is quite obvious that the interpretation sought bears no relation to the actual facts of the main action or to its purposes or where the problem is hypothetical or the Court does not have before it the factual or legal material necessary to give a useful answer to the question submitted to it (judgment of 4 May 2023,   
Österreichische Post (Non-material damage in connection with the processing of personal data)  
, C-300/21, EU:C:2023:370, paragraph 23 and the case-law cited).  
30      In the present case, the first question concerns the conditions required for the exercise of the right to compensation provided for in Article 82 of the GDPR. Furthermore, it is not obvious that the interpretation sought bears no relation to the dispute in the main proceedings or that the problem raised is hypothetical. This dispute concerns a claim for compensation falling within the rules established by the GDPR for the protection of personal data. Second, that question seeks, in essence, to determine whether, for the purposes of the application of the rules on liability laid down by that regulation, it is necessary not only that there be non-material damage that is distinct from the infringement of that regulation, but also that that damage exceeds a certain threshold of seriousness.  
31      The first question is therefore admissible.  
   
Substance  
32      By its first question, the referring court asks, in essence, whether Article 82(1) of the GDPR must be interpreted as meaning that an infringement of provisions of that regulation which confer rights on the data subject is sufficient, in itself, to constitute ‘non-material damage’, within the meaning of that provision, irrespective of the degree of seriousness of the harm suffered by that person.  
33      As a preliminary point, it should be recalled that Article 82(1) GDPR provides that any person ‘who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered’.  
34      The Court has already interpreted Article 82(1) of the GDPR as meaning that the mere infringement of that regulation is not sufficient to confer a right to compensation, since the existence of ‘damage’, material or non-material, or of ‘damage’ which has been ‘suffered’ constitutes one of the conditions for the right to compensation laid down in Article 82(1), as does the existence of an infringement of that regulation and of a causal link between that damage and that infringement, those three conditions being cumulative (see, to that effect, judgment of 25 January 2024,   
MediaMarktSaturn  
, C-687/21, EU:C:2024:72, paragraph 58 and the case-law cited).  
35      Thus, the person seeking compensation for non-material damage on the basis of that provision is required to establish not only the infringement of provisions of that regulation, but also that that infringement caused him or her such damage (see, to that effect, judgment of 25 January 2024,   
MediaMarktSaturn  
 (C-687/21, EU:C:2024:72, paragraphs 60 and 61 and the case-law cited).  
36      On that point, it should be noted that the Court has interpreted Article 82(1) of the GDPR as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness, while emphasising that that person is nevertheless required to demonstrate that the infringement of that regulation caused him or her such non-material damage (see, to that effect, judgment of 25 January 2024,   
MediaMarktSaturn,  
 C-687/21, EU:C:2024:72, paragraphs 59 and 60 and the case-law cited).  
37      Even if the provision of the GDPR which has been infringed grants rights to natural persons, such an infringement cannot, in itself, constitute ‘non-material damage’ within the meaning of that regulation.  
38      Admittedly, it is apparent from Article 79(1) of the GDPR that every data subject has the right to an effective judicial remedy against the controller or any processor if he or she considers that ‘his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation’.  
39      However, that provision merely confers a right to bring an action on a person who considers himself or herself to be a victim of a breach of the rights conferred on him or her by the GDPR, without exempting that person from his or her obligation under Article 82(1) of that regulation to prove that he or she has actually suffered material or non-material damage.  
40      It follows that the infringement of provisions of the GDPR granting rights to the data subject is not in itself sufficient to found a substantive right to obtain compensation under that regulation, which requires that the other two conditions of that right referred to in paragraph 34 of the present judgment also be satisfied.  
41      In the present case, the applicant in the main proceedings claims, on the basis of the GDPR, compensation for non-material damage, namely a loss of control over his personal data that have been processed despite his objection, without being required to prove that that damage exceeded a certain threshold of seriousness.  
42      In that regard, it should be noted that recital 85 of the GDPR expressly mentions ‘loss of control’ among the damage that may be caused by a personal data breach. In addition, the Court has held that the loss of control over such data, even for a short period of time, may constitute ‘non-material damage’, within the meaning of Article 82(1) of that regulation, giving rise to a right to compensation, provided that the data subject can show that he or she has actually suffered such damage, however slight (see, to that effect, judgment of 25 January 2024 in   
MediaMarktSaturn  
, C-687/21, EU:C:2024:72, paragraph 66 and the case-law cited).  
43      In the light of the foregoing reasons, the answer to the first question is that Article 82(1) of the GDPR must be interpreted as meaning that an infringement of provisions of that regulation which confer rights on the data subject is not sufficient, in itself, to constitute ‘non-material damage’ within the meaning of that provision, irrespective of the degree of seriousness of the damage suffered by that person.  
   
The second question  
44      By its second question, the referring court asks, in essence, whether Article 82 of the GDPR must be interpreted as meaning that it is sufficient for the controller, in order to be exempted from liability under paragraph 3 of that article, to claim that the damage in question was caused by the failure of a person acting under his authority, within the meaning of Article 29 of that regulation.  
45      In that regard, it should be recalled that Article 82 of the GDPR states, in paragraph 2 thereof, that any controller involved in the processing is to be liable for the damage caused by processing which infringes that regulation and, in paragraph 3 thereof, that a controller is exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.  
46      The Court has already held that it is apparent from a combined analysis of Article 82(2) and (3) that that article provides for a fault-based regime, in which the controller is presumed to have participated in the processing constituting the breach of the GDPR in question, so that the burden of proof lies not with the person who has suffered damage but with the controller (see, to that effect, judgment of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraphs 92 to 94).  
47      As regards whether the controller may be exempted from liability under Article 82(3) of the GDPR on the sole ground that that damage was caused by the wrongful conduct of a person acting under his authority, within the meaning of Article 29 of that regulation, first, it is apparent from Article 29 that persons acting under the authority of the controller, such as its employees, who have access to personal data, may, in principle, process those data only on instructions from that controller and in accordance with those instructions (see, to that effect, judgment of 22 June 2023,   
Pankki S  
, C-579/21, EU:C:2023:501, paragraphs 73 and 74).  
48      Second, Article 32(4) of the GDPR, relating to the security of processing of personal data, provides that the controller is to take steps to ensure that any natural person acting under the authority of the controller, who has access to such data, does not process them, except on instructions from the controller, unless he or she is required to do so by EU or Member State law.  
49      An employee of the controller is indeed a natural person acting under the authority of that controller. Thus, it is for that controller to ensure that his or her instructions are correctly applied by his or her employees. Accordingly, the controller cannot avoid liability under Article 82(3) of the GDPR simply by relying on negligence or failure on the part of a person acting under his or her authority.  
50      In the present case, in its written observations before the Court, juris submits, in essence, that the controller should be exempt from liability under Article 82(3) of the GDPR where the breach which caused the damage in question is attributable to the conduct of one of its employees who has failed to comply with the instructions of that controller and provided that that breach is not due to a failure to comply with the obligations of the controller set out, in particular, in Articles 24, 25 and 32 of that regulation.  
51      In that regard, it must be pointed out that the circumstances of the exemption provided for in Article 82(3) of the GDPR must be strictly limited to those in which the controller is able to demonstrate that the damage is not attributable to him or her (see, to that effect, judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraph 70). Therefore, in the event of a personal data breach committed by a person acting under his or her authority, that controller may benefit from that exemption only if he or she proves that there is no causal link between any breach of the data protection obligation incumbent on him or her under Articles 5, 24 and 32 of that regulation and the damage suffered by the data subject (see, by analogy, judgment of 14 December 2023,   
Natsionalna agentsia za prihodite  
, C-340/21, EU:C:2023:986, paragraph 72).  
52      Therefore, in order for the controller to be exempted from liability under Article 82(3) of the GDPR, it cannot be sufficient for him or her to demonstrate that he or she had given instructions to persons acting under its authority, within the meaning of Article 29 of that regulation, and that one of those persons failed in his or her obligation to follow those instructions, with the result that that person contributed to the occurrence of the damage in question.  
53      If it were accepted that the controller may be exempted from liability merely by relying on the failure of a person acting under his or her authority, that would undermine the effectiveness of the right to compensation enshrined in Article 82(1) of the GDPR, as the referring court noted, in essence, and would not be consistent with the objective of that regulation, which is to ensure a high level of protection for individuals with regard to the processing of their personal data.  
54      In the light of the foregoing, the answer to the second question is that Article 82 of the GDPR must be interpreted as meaning that it is not sufficient for the controller, in order to be exempted from liability under paragraph 3 of that article, to claim that the damage in question was caused by the failure of a person acting under his or her authority, within the meaning of Article 29 of that regulation.  
   
The third and fourth questions  
55      By its third and fourth questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 82(1) of the GDPR must be interpreted as meaning that, in order to determine the amount of damages due as compensation for damage based on that provision, it is necessary, first, to apply   
mutatis mutandis  
 the criteria for setting the amount of administrative fines laid down in Article 83 of that regulation and, second, to take account of the fact that several infringements of that regulation concerning the same processing operation affect the person seeking compensation.  
56      In the first place, as regards the possible taking into account of the criteria set out in Article 83 of the GDPR for the purpose of assessing the amount of compensation due under Article 82 thereof, it is common ground that those two provisions pursue different objectives. While Article 83 of that regulation determines the ‘general conditions for imposing administrative fines’, Article 82 of that regulation governs the ‘right to compensation and liability’.  
57      It follows that the criteria set out in Article 83 of the GDPR for the purposes of determining the amount of administrative fines, which are also mentioned in recital 148 of that regulation, cannot be used to assess the amount of damages under Article 82 thereof.  
58      As the Court has already pointed out, the GDPR does not contain any provision relating to the assessment of the damages due under the right to compensation enshrined in Article 82 of that regulation. Therefore, for the purposes of that assessment, the national courts must, in accordance with the principle of procedural autonomy, apply the domestic rules of each Member State relating to the extent of monetary compensation, provided that the principles of equivalence and effectiveness of EU law, as defined by the settled case-law of the Court, are complied with (see, to that effect, judgments of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraphs 83 and 101 and the case-law cited, and of 25 January 2024,   
MediaMarktSaturn  
, C-687/21, EU:C:2024:72, paragraph 53).  
59      In that context, the Court emphasised that Article 82 of the GDPR has a function that is compensatory and not punitive, contrary to other provisions of that regulation also contained in Chapter VIII thereof, namely Articles 83 and 84, which have, for their part, essentially a punitive purpose, since they permit the imposition of administrative fines and other penalties, respectively. The relationship between the rules set out in Article 82 and those set out in Articles 83 and 84 shows that there is a difference between those two categories of provisions, but also complementarity, in terms of encouraging compliance with the GDPR, it being observed that the right of any person to seek compensation for damage reinforces the operational nature of the protection rules laid down by that regulation and is likely to discourage the reoccurrence of unlawful conduct (judgment of 25 January 2024,   
MediaMarktSaturn  
, C-687/21, EU:C:2024:72, paragraph 47 and the case-law cited).  
60      Furthermore, the Court inferred from the fact that the right to compensation provided for in Article 82(1) of the GDPR does not fulfil a deterrent, or even punitive, function that the gravity of the infringement of that regulation that caused the alleged material or non-material damage cannot influence the amount of the compensation granted under that provision. It follows that that amount cannot exceed the full compensation for that damage (see, to that effect, judgment of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraph 86).  
61      Referring to the sixth sentence of recital 146 of the GDPR, according to which that instrument is intended to ensure ‘full and effective compensation for the damage … suffered’, the Court noted that, in view of the compensatory function of the right to compensation provided for in Article 82 of that regulation, monetary compensation based on that article must be regarded as ‘full and effective’ if it allows the damage actually suffered as a result of the infringement of that regulation to be compensated in its entirety, without there being any need, for the purposes of such compensation for the damage in its entirety, to require the payment of punitive damages (judgment of 21 December 2023,   
Krankenversicherung Nordrhein  
, C-667/21, EU:C:2023:1022, paragraph 84 and the case-law cited).  
62      Thus, in the light of the differences in wording and purposes existing between Article 82 of the GDPR, read in the light of recital 146 thereof, and Article 83 of that regulation, read in the light of recital 148 thereof, it cannot be considered that the assessment criteria set out specifically in Article 83 are applicable   
mutatis mutandis  
 in the context of Article 82, notwithstanding the fact that the legal remedies provided for in those two provisions are indeed complementary to ensure compliance with that regulation.  
63      In the second place, as regards the way in which national courts must assess the amount of monetary compensation under Article 82 of the GDPR in the case of multiple infringements of that regulation affecting the same data subject, it should, first of all, be pointed out that, as mentioned in paragraph 58 of the present judgment, it is for each Member State to establish the criteria for determining the amount of that compensation, subject to compliance with the principles of effectiveness and equivalence of EU law.  
64      Next, in view of the compensatory rather than punitive function of Article 82 of the GDPR, which is recalled in paragraphs 60 and 61 of this judgment, the fact that several infringements have been committed by the controller in relation to the same data subject cannot constitute a relevant criterion for the purposes of assessing the compensation to be awarded to that data subject under Article 82. Only the damage actually suffered by that person must be taken into consideration in order to determine the amount of the monetary compensation due by way of compensation.  
65      Consequently, the answer to the third and fourth questions is that Article 82(1) of the GDPR must be interpreted as meaning that, in order to determine the amount of damages due as compensation for damage based on that provision, it is not necessary, first, to apply   
mutatis mutandis  
 the criteria for setting the amount of administrative fines laid down in Article 83 of that regulation and, second, to take account of the fact that several infringements of that regulation concerning the same processing operation affect the person seeking compensation.  
   
Costs  
66      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 82(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
must be interpreted as meaning that an infringement of provisions of that regulation which confer rights on the data subject is not sufficient, in itself, to constitute ‘non-material damage’ within the meaning of that provision, irrespective of the degree of seriousness of the damage suffered by that person.  
2.        
Article 82 of Regulation 2016/679  
must be interpreted as meaning that it is not sufficient for the controller, in order to be exempted from liability under paragraph 3 of that article, to claim that the damage in question was caused by the failure of a person acting under his or her authority, within the meaning of Article 29 of that regulation.  
3.        
Article 82(1) of Regulation 2016/679  
must be interpreted as meaning that in order to determine the amount of damages due as compensation for damage based on that provision, it is not necessary, first, to apply   
mutatis mutandis  
 the criteria for setting the amount of administrative fines laid down in Article 83 of that regulation and, second, to take account of the fact that several infringements of that regulation concerning the same processing operation affect the person seeking compensation.

ID: c377ce10-7b04-4777-ab84-f4c25291d5bf

Judgment of 22 Nov 2012, C-119/12 (  
Probst  
)  
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Data processor agreement   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Security of processing   
   
JUDGMENT OF THE COURT (Third Chamber)  
22 November 2012 (\*)  
(Electronic communications – Directive 2002/58/EC – Article 6(2) and (5) – Processing of personal data – Traffic data necessary for billing and debt collection – Debt collection by a third company – Persons acting under the authority of the providers of public communications networks and electronic communications services)  
In Case C-119/12,  
REFERENCE for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Germany), made by decision of 16 February 2012, received at the Court on 6 March 2012, in the proceedings  
Josef Probst  
v  
mr.nexnet GmbH,  
THE COURT (Third Chamber),  
composed of K. Lenaerts (Rapporteur), acting as President of the Third Chamber, E. Juhász, G. Arestis, T. von Danwitz and D. Šváby, Judges,  
Advocate General: P. Cruz Villalón,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,   
after considering the observations submitted on behalf of:  
–        mr.nexnet GmbH, by P. Wassermann, Rechtsanwalt,  
–        the European Commission, by F. Wilman and F. Bulst, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This reference for a preliminary ruling concerns the interpretation of Article 6(2) and (5) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).  
2        The reference has been made in proceedings between mr.nexnet GmbH (‘nexnet’), the assignee of claims for payment for the supply of internet access services by Verizon Deutschland GmbH (‘Verizon’), and Mr Probst, the recipient of those services.  
   
Legal context  
   
Directive 95//46/EC  
3        Article 16 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) provides:  
‘Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.’  
4        Article 17 of Directive 95/46 provides:  
‘1.      Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.  
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.  
2.      The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.   
3.      The carrying-out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:  
–        the processor shall act only on instructions from the controller,  
–        the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.  
4.      For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.’  
   
Directive 2002/58/EC  
5        Article 1(1) and (2) of Directive 2002/58 provides:  
‘1.      This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the [European Union].  
2.      The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. …’  
6        Point b of the second paragraph of Article 2 of that directive defines ‘traffic data’ as ‘any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof’.  
7        Article 5(1) of Directive 2002/58 states:  
‘Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. …’  
8        Article 6 of that directive provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article ...  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
…’  
   
German law  
9        The third and fourth sentences of Paragraph 97(1) of the Law on telecommunications (Telekommunikationsgesetz) of 22 June 2004 (BGBl. 2004 I, p. 1190; the ‘TKG’) are worded as follows:  
‘Determination and billing of the provider’s remuneration  
… If the service provider has concluded a contract with a third party relating to the collection of the charges for service, it is entitled to pass on the [traffic] data in so far as that data transfer is necessary for the collection of charges and for drawing up a detailed bill. The third party must be contractually bound with respect to privacy of telecommunications in accordance with Paragraph 88 and with respect to data protection in accordance with Paragraphs 93, 95, 96, 97, 99 and 100.  
…’   
10      According to the referring court, the authorisation provided for in the third sentence of Paragraph 97(1) of the TKG on passing on data applies not only to debt collection contracts where those debts remain part of the property of the original holder, but also to other contracts for assignment, in particular contracts for the purchase of debts, and which provide that the right assigned belongs definitively to the assignee both in legal and economic terms.  
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
11      Mr Probst is the owner of a telephone line provided by Deutsche Telekom AG, through which his computer is connected to the internet. From 28 June 2009 to 6 September 2009, he used the number provide by Verizon to obtain occasional access to the internet. At first, the charges claimed for were billed to Mr Probst by Deutsche Telekom AG as ‘amounts due to other providers’. When Mr Probst failed to make payment, nexnet, as assignee of that debt pursuant to a factoring contract concluded between the legal predecessors to Verizon and to nexnet, claimed payment of the amounts billed together with various charges. Under the factoring contract nexnet bears the risk of debtor default.  
12      The legal predecessors of nexnet and Verizon also concluded a ‘data protection and confidentiality agreement’ which provides:  
‘I      Data protection  
…  
(5)      The contracting parties undertake to process and use the protected data only within the framework of the abovementioned cooperation and exclusively for the purpose of the present contract and in the manner prescribed.  
(6)      As soon as the information included as protected data is no longer required for such purpose, all protected data held in that connection shall forthwith be erased irretrievably or returned. …  
(7)      Each contracting party shall be entitled to check that the other party has ensured data protection and data security in accordance with the present agreement. …  
II. Confidentiality  
…  
(2)      The contracting parties shall process and use the confidential documents and information provided exclusively for the performance of the contract concluded between them. They shall make these accessible only to those employees who require such for the performance of the contract. The parties shall require those employees to maintain confidentiality in accordance with this agreement.  
(3)      On request by a contracting party, or at the latest on termination of the cooperation between the contracting parties, all confidential data held in that connection shall be erased irretrievably or returned to the other party. …  
…’  
13      According to Mr Probst, the factoring contract is void in so far as it breaches, inter alia, Paragraph 97(1) of the TKG. The Amtsgericht (local court) rejected nexnet’s claim for payment, while the appellate court upheld it in substance. An appeal on a point of law (‘Revision’) has been brought before the Bundesgerichtshof (Federal Court of Justice).  
14      The Bundesgerichtshof takes the view that Article 6(2) and (5) of Directive 2002/58 is relevant for the interpretation of Paragraph 97(1) of the TKG. It states, first, that ‘billing’, which is one of the objectives in respect of which Article 6(2) and (5) of that directive authorises the processing of traffic data, does not necessarily include the collection of the amount invoiced. However, it takes the view there is no objective reason for treating billing and debt collection differently with respect to data protection. Second, Article 6(5) of that directive restricts the processing of traffic data to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services (‘service provider’). According to the referring court, it is unclear from that definition whether the service provider must actually be able to determine the use of the data, including on a case-by-case basis, throughout the duration of the data processing or whether it is sufficient that general rules relating to respect for the privacy of telecommunications and data protection are laid down, such as those agreed in the present case in the contractual provisions, and that it is possible for the data to be erased or returned on request.  
15      In those circumstances, the Bundesgerichtshof decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
‘Does Article 6(2) and (5) of Directive 2002/58 permit the passing of traffic data from the service provider to the assignee of a claim for payment in respect of telecommunications services in the case where the assignment effected with a view to the collection of transferred debts includes, in addition to the general obligation to respect the privacy of telecommunications and to ensure data protection as provided for under the applicable legislation, the following contractual stipulations:   
–        the service provider and the assignee undertake to process and use the protected data only within the framework of their cooperation and exclusively for the purpose of the contract and in the manner prescribed therein;   
–        as soon as the information in the protected data is no longer required for such purpose, all protected data held in that connection are to be irreversibly erased or returned;   
–        each contracting party is entitled to check that the other party has ensured data protection and data security in accordance with this agreement;  
–        confidential documents and information transferred may be made accessible only to such employees as require these for the purposes of performing the contract;  
–        the contracting parties are to require those employees to maintain confidentiality in accordance with this agreement;  
–        on request, or at the latest on termination of the cooperation between the contracting parties, all confidential data held in that connection are to be irreversibly erased or returned to the other party?’  
   
Consideration of the question referred for a preliminary ruling  
16      By its question, the referring court asks essentially whether, and in what circumstances, Article 6(2) and (5) of Directive 2002/58 allows a service provider to pass traffic data to the assignee of its claims for payment and allows the latter to process those data.  
17      First, in accordance with Article 6(2) of Directive 2002/58, traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. As nexnet and the European Commission submit, that provision of that directive authorises processing of traffic data not only for the purpose of billing but also for that of debt collection. By authorising traffic data processing ‘up to the end of the period during which the bill may lawfully be challenged or payment pursued’, that provision relates not only to data processing at the time of billing but also to the processing necessary for securing payment thereof.  
18      Second, pursuant to Article 6(5) of Directive 2002/58, traffic data processing authorised by Article 6(2) thereof ‘must be restricted to persons acting under the authority of [service] providers of the public communications networks and publicly available electronic communications services handling billing’ and ‘must be restricted to what is necessary’ for the purposes of such an activity.  
19      It follows from a combined reading of those provisions of Directive 2002/58 that a service provider is authorised to pass traffic data to the assignee of its claims for payment for the purpose of their recovery and that the latter is authorised to process those data on condition, first, that it acts ‘under the authority’ of the service provider as regards the processing of those data and, second, that it processes only traffic data which are necessary for the purpose of the recovery of those claims.  
20      It must be stated that neither Directive 2002/58 nor the documents relevant for its interpretation, such as the   
travaux préparatoires  
, provide clarification as to the exact scope of the concept of ‘under the authority’. The meaning and scope of terms for which European Union law provides no definition must be determined by considering their usual meaning in everyday language, while also taking into account the context in which they occur and the purposes of the rules of which they are part (see, to that effect, judgments in Case C-336/03   
easyCar  
 [2005] ECR I-1947, paragraphs 20 and 21, and of 5 July 2012 in Case C-49/11   
Content Services  
, paragraph 32).  
21      As regards the usual meaning of those words in everyday language, it must be held that a persons acts under the authority of another where the former acts on instructions and under the control of the latter.  
22      As to the context in which Article 6 of Directive 2002/58 appears, it must be recalled that Article 5(1) of that directive provides that Member States are required to ensure the confidentiality of communications by means of a public communications network and publicly available electronic communications services and the related traffic data.  
23      Article 6(2) and (5) of Directive 2002/58 contains an exception to the confidentiality of communications laid down in Article 5(1) by authorising traffic data processing in accordance with the requirements of billing services (see, to that effect, Case C-275/06   
Promusicae  
 [2008] ECR I-271, paragraph 48). As it constitutes an exception, that provision of that directive, and therefore also the words ‘under the authority’, are to be interpreted strictly (see Case C-16/10   
The Number (UK) and Conduit Enterprises  
 [2011] ECR I-691, paragraph 31). Such an interpretation requires that the service provider has an actual power of supervision which enables him to determine whether the assignee of the claims for payment is acting in compliance with the conditions imposed on it with respect to the processing of traffic data.  
24      That interpretation is corroborated by the objective of Directive 2002/58 in general and of Article 6(5) in particular. As is clear from its Article 1(1) and (2), Directive 2002/58 particularises and complements Directive 95/46 in the electronic communications sector for the purposes, inter alia, of ensuring an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communications sector.  
25      In those circumstances, Article 6(5) of Directive 2002/58 must be interpreted in the light of similar provisions in Directive 95/46. It is clear from Articles 16 and 17 of Directive 95/46, which set out the level of control that the controller must exercise over the processor which it appoints, that that processor acts only on the controller’s instructions and that the controller ensures compliance with the measures agreed in order to protect personal data against any form of unlawful processing.  
26      As regards the objective pursued by Article 6(5) of Directive 2002/58 in particular, it must be stated that, even if that provision authorises the processing of traffic data by certain third persons for the service supplier for the purpose in particular of collecting the latter’s debts, thereby enabling it to concentrate on the supply of electronic communications services, that provision seeks to ensure, by providing that the processing of traffic data must be restricted to persons acting ‘under the control’ of the service supplier, that such externalisation does not affect the level of protection of personal data enjoyed by the user.  
27      It follows from the foregoing that, regardless of the classification of the contract of assignment of claims for payment for collection purposes, the assignee of a claim for payment relating to the payment of telecommunications charges acts ‘under the authority’ of the service provider, within the meaning of Article 6(5) of Directive 2002/58, where, for the processing of traffic data that such an activity involves, the assignee acts only on instructions and under the control of the service provider. In particular, the contract concluded between the service provider which assigns its claims for payment and the party to which those claims are assigned must contain provisions of such a kind as to ensure the lawful processing of traffic data by the latter and must allow the service provider to ensure at all times that those provisions are being complied with by the assignee.  
28      It is for the national court to determine, in the light of all the information in the case-file, whether those conditions are met in the case in the main proceedings. The fact that a factoring contract has the characteristics described in the question referred suggests that that contract satisfies those conditions. Such a contract allows the processing of traffic data by the assignee of claims for payment only in so far as such processing is necessary for the collection of those debts and imposes on that assignee the obligation immediately and irreversibly to erase or return those data as soon as knowledge thereof is no longer necessary for the recovery of the claims concerned. Furthermore, it allows the service provider to check whether there is compliance with the rules on security and data protection on the part of the assignee, which may, on simple request, be obliged to erase or to return the traffic data.  
29      In the light of the foregoing, the answer to the question referred is that Article 6(2) and (5) of Directive 2002/58 must be interpreted as authorising a service provider to pass traffic data to the assignee of its claims for payment in respect of the supply of telecommunications services for the purpose of recovery of those claims, and as authorising that assignee to process those data on condition, first, that it acts under the authority of the service provider as regards the processing of those data and, second, that that assignee confines itself to processing the traffic data necessary for the purposes of recovering the claims assigned.  
30      Irrespective of the classification of the contract of assignment, the assignee is deemed to act under the authority of the service provider, within the meaning of Article 6(5) of Directive 2002/58, where, for the processing of traffic data, it acts exclusively on the instructions and under the control of that provider. In particular, the contract concluded between them must contain provisions capable of guaranteeing the lawful processing, by the assignee, of the traffic data and of enabling the service provider to ensure, at all times, that that assignee is complying with those provisions.  
   
Costs  
31      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Article 6(2) and (5) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) must be interpreted as authorising a provider of public communications networks and of publicly-accessible electronic communications services to pass traffic data to the assignee of its claims for payment in respect of the supply of telecommunications services for the purpose of recovery of those claims, and as authorising that assignee to process those data on condition, first, that the latter acts under the authority of the service provider as regards the processing of those data and, second, that that assignee confines itself to processing the traffic data necessary for the purposes of recovering the claims assigned.  
Irrespective of the classification of the contract of assignment, the assignee is deemed to act under the authority of the service provider, within the meaning of Article 6(5) of Directive 2002/58, where, for the processing of traffic data, it acts exclusively on the instructions and under the control of that provider. In particular, the contract concluded between them must contain provisions capable of guaranteeing the lawful processing, by the assignee, of the traffic data and of enabling the service provider to ensure, at all times, that that assignee is complying with those provisions.

ID: c3ed25f3-3397-4234-827c-eaa6c9509bfa

Judgment of 24 Nov 2011, C-70/10 (  
Scarlet Extended  
)  
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
E-privacy Directive   
 >   
Electronic communications   
 >   
Confidentiality of electronic communications   
   
JUDGMENT OF THE COURT (Third Chamber)  
24 November 2011 (\*)  
(Information society – Copyright – Internet – ‘Peer-to-peer’ software – Internet service providers – Installation of a system for filtering electronic communications in order to prevent file sharing which infringes copyright – No general obligation to monitor information transmitted)  
In Case C-70/10,  
REFERENCE for a preliminary ruling under Article 267 TFEU from the cour d’appel de Bruxelles (Belgium), made by decision of 28 January 2010, received at the Court on 5 February 2010, in the proceedings  
Scarlet Extended SA  
v  
Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),  
intervening parties:  
Belgian Entertainment Association Video ASBL (BEA Video),  
Belgian Entertainment Association Music ASBL (BEA Music),  
Internet Service Provider Association ASBL (ISPA),  
THE COURT (Third Chamber),  
composed of K. Lenaerts, President of the Chamber, J. Malenovský (Rapporteur), R. Silva de Lapuerta, E. Juhász and G. Arestis, Judges,  
Advocate General: P. Cruz Villalón,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 13 January 2011,  
after considering the observations submitted on behalf of:  
–        Scarlet Extended SA, by T. De Meese and B. Van Asbroeck, avocats,  
–        Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Belgian Entertainment Association Video ASBL (BEA Video) and Belgian Entertainment Association Music ASBL (BEA Music), by F. de Visscher, B. Michaux and F. Brison, avocats,  
–        Internet Service Provider Association ASBL (ISPA), by G. Somers, avocat,  
–        the Belgian Government, by T. Materne, J.-C. Halleux and C. Pochet, acting as Agents,  
–        the Czech Government, by M. Smolek and K. Havlíčková, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, assisted by S. Fiorentino, avvocato dello Stato,  
–        the Netherlands Government, by C. Wissels and B. Koopman, acting as Agents,  
–        the Polish Government, by M. Szpunar, M. Drwięcki and J. Goliński, acting as Agents,  
–        the Finnish Government, by M. Pere, acting as Agent,  
–        the European Commission, by J. Samnadda and C. Vrignon, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 14 April 2011,  
gives the following  
Judgment  
1        This reference for a preliminary ruling concerns the interpretation of Directives:  
–        2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) (OJ 2000 L 178, p. 1);   
–        2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10);  
–        2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum OJ 2004 L 195, p. 16);   
–        95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31); and   
–        2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).  
2        The reference has been made in proceedings between Scarlet Extended SA (‘Scarlet’) and the Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (‘SABAM’) concerning Scarlet’s refusal to install a system for filtering electronic communications which use file-sharing software (‘peer-to-peer’), with a view to preventing file sharing which infringes copyright.  
   
Legal context  
   
European Union law  
 Directive 2000/31  
3        Recitals 45 and 47 in the preamble to Directive 2000/31 state:  
‘(45)      The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.  
…  
(47)      Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.’   
4        Article 1 of Directive 2000/31 states:  
‘1.      This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.  
2.      This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.  
…’  
5        Article 12 of that directive, which features in Section 4, entitled ‘Liability of intermediary service providers’, of Chapter II thereof, provides:  
‘1.      Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:  
(a)      does not initiate the transmission;  
(b)      does not select the receiver of the transmission; and  
(c)      does not select or modify the information contained in the transmission.  
…  
3.      This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement.’  
6        Article 15 of Directive 2000/31, which also features in Section 4 of Chapter II, states:  
‘1.      Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating unlawful activity.  
2.      Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged unlawful activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.’  
 Directive 2001/29  
7        Recitals 16 and 59 in the preamble to Directive 2001/29 state:  
‘(16)      … This Directive should be implemented within a timescale similar to that for the implementation of [Directive 2000/31], since that Directive provides a harmonised framework of principles and provisions relevant, inter alia, to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive.  
...  
(59)      In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party’s infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.’   
8        Article 8 of Directive 2001/29 states:  
‘1.      Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.  
…  
3.      Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.’  
 Directive 2004/48  
9        Recital 23 in the preamble to Directive 2004/48 provides:  
‘Without prejudice to any other measures, procedures and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary whose services are being used by a third party to infringe the rightholder’s industrial property right. The conditions and procedures relating to such injunctions should be left to the national law of the Member States. As far as infringements of copyright and related rights are concerned, a comprehensive level of harmonisation is already provided for in Directive [2001/29]. Article 8(3) of Directive [2001/29] should therefore not be affected by this Directive.’  
10      Article 2(3) of Directive 2004/48 provides as follows:  
‘This Directive shall not affect:  
(a)       the Community provisions governing the substantive law on intellectual property … or Directive [2000/31], in general, and Articles 12 to 15 of Directive [2000/31] in particular;  
…’  
11      Article 3 of Directive 2004/48 provides:  
‘1.      Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.  
2.      Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.’  
12      Article 11 of Directive 2004/48 states:  
‘Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive [2001/29].’  
   
National law  
13      Article 87(1), first and second subparagraphs, of the Law of 30 June 1994 on copyright and related rights (  
Moniteur belge   
of 27 July 1994, p. 19297) states:   
‘The President of the Tribunal de première instance (Court of First Instance) … shall determine the existence of any infringement of a copyright or related right and shall order that it be brought to an end.  
He may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.’   
14      Articles 18 and 21 of the Law of 11 March 2003 on certain legal aspects of information society services (  
Moniteur belge   
of 17 March 2003, p. 12962) transpose Articles 12 and 15 of Directive 2000/31 into national law.   
   
The dispute in the main proceedings and the questions referred for a preliminary ruling   
15      SABAM is a management company which represents authors, composers and editors of musical works in authorising the use of their copyright-protected works by third parties.   
16      Scarlet is an internet service provider (‘ISP’) which provides its customers with access to the internet without offering other services such as downloading or file sharing.   
17      In the course of 2004, SABAM concluded that internet users using Scarlet’s services were downloading works in SABAM’s catalogue from the internet, without authorisation and without paying royalties, by means of peer-to-peer networks, which constitute a transparent method of file sharing which is independent, decentralised and features advanced search and download functions.   
18      On 24 June 2004, SABAM accordingly brought interlocutory proceedings against Scarlet before the President of the Tribunal de première instance, Brussels, claiming that that company was the best placed, as an ISP, to take measures to bring to an end copyright infringements committed by its customers.   
19      SABAM sought, first, a declaration that the copyright in musical works contained in its repertoire had been infringed, in particular the right of reproduction and the right of communication to the public, because of the unauthorised sharing of electronic music files by means of peer-to-peer software, those infringements being committed through the use of Scarlet’s services.  
20      SABAM also sought an order requiring Scarlet to bring such infringements to an end by blocking, or making it impossible for its customers to send or receive in any way, files containing a musical work using peer-to-peer software without the permission of the rightholders, on pain of a periodic penalty. Lastly, SABAM requested that Scarlet provide it with details of the measures that it would be applying in order to comply with the judgment to be given, on pain of a periodic penalty.  
21      By judgment of 26 November 2004, the President of the Tribunal de première instance, Brussels, found that copyright had been infringed, as claimed by SABAM, but, prior to ruling on the application for cessation, appointed an expert to investigate whether the technical solutions proposed by SABAM were technically feasible, whether they would make it possible to filter out only unlawful file sharing, and whether there were other ways of monitoring the use of peer-to-peer software, and to determine the cost of the measures envisaged.  
22      In his report, the appointed expert concluded that, despite numerous technical obstacles, the feasibility of filtering and blocking the unlawful sharing of electronic files could not be entirely ruled out.   
23      By judgment of 29 June 2007, the President of the Tribunal de première instance, Brussels, accordingly ordered Scarlet to bring to an end the copyright infringements established in the judgment of 26 November 2004 by making it impossible for its customers to send or receive in any way files containing a musical work in SABAM’s repertoire by means of peer-to-peer software, on pain of a periodic penalty.   
24      Scarlet appealed against that decision to the referring court, claiming, first, that it was impossible for it to comply with that injunction since the effectiveness and permanence of filtering and blocking systems had not been proved and that the installation of the equipment for so doing was faced with numerous practical obstacles, such as problems with the network capacity and the impact on the network. Moreover, any attempt to block the files concerned was, it argued, doomed to fail in the very short term because there were at that time several peer-to-peer software products which made it impossible for third parties to check their content.  
25      Scarlet also claimed that that injunction was contrary to Article 21 of the Law of 11 March 2003 on certain legal aspects of information society services, which transposes Article 15 of Directive 2000/31 into national law, because it would impose on Scarlet,   
de facto  
, a general obligation to monitor communications on its network, inasmuch as any system for blocking or filtering peer-to-peer traffic would necessarily require general surveillance of all the communications passing through its network.  
26      Lastly, Scarlet considered that the installation of a filtering system would be in breach of the provisions of European Union law on the protection of personal data and the secrecy of communications, since such filtering involves the processing of IP addresses, which are personal data.   
27      In that context, the referring court took the view that, before ascertaining whether a mechanism for filtering and blocking peer-to-peer files existed and could be effective, it had to be satisfied that the obligations liable to be imposed on Scarlet were in accordance with European Union law.   
28      In those circumstances, the cour d’appel de Bruxelles decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Do Directives 2001/29 and 2004/48, in conjunction with Directives 95/46, 2000/31 and 2002/58, construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: ‘They [the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right’, to order an [ISP] to install, for all its customers, in abstracto and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent?  
(2)      If the answer to the [first] question … is in the affirmative, do those directives require a national court, called upon to give a ruling on an application for an injunction against an intermediary whose services are used by a third party to infringe a copyright, to apply the principle of proportionality when deciding on the effectiveness and dissuasive effect of the measure sought?’  
   
Consideration of the questions referred  
29      By its questions, the referring court asks, in essence, whether Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction imposed on an ISP to introduce a system for filtering  
–        all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;   
–        which applies indiscriminately to all its customers;   
–        as a preventive measure;   
–        exclusively at its expense; and  
–        for an unlimited period,   
which is capable of identifying on that provider’s network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual property rights, with a view to blocking the transfer of files the sharing of which infringes copyright (‘the contested filtering system’).  
30      In that regard, it should first be recalled that, under Article 8(3) of Directive 2001/29 and the third sentence of Article 11 of Directive 2004/48, holders of intellectual property rights may apply for an injunction against intermediaries, such as ISPs, whose services are being used by a third party to infringe their rights.  
31      Next, it follows from the Court’s case-law that the jurisdiction conferred on national courts, in accordance with those provisions, must allow them to order those intermediaries to take measures aimed not only at bringing to an end infringements already committed against intellectual-property rights using their information-society services, but also at preventing further infringements (see, to that effect, Case C-324/09   
L’Oréal and Others   
[2011] ECR I-0000, paragraph 131).  
32      Lastly, it follows from that same case-law that the rules for the operation of the injunctions for which the Member States must provide under Article 8(3) of Directive 2001/29 and the third sentence of Article 11 of Directive 2004/48, such as those relating to the conditions to be met and to the procedure to be followed, are a matter for national law (see,   
mutatis mutandis  
,   
L’Oréal and Others  
, paragraph 135).   
33      That being so, those national rules, and likewise their application by the national courts, must observe the limitations arising from Directives 2001/29 and 2004/48 and from the sources of law to which those directives refer (see, to that effect,   
L’Oréal and Others  
, paragraph 138).   
34      Thus, in accordance with recital 16 in the preamble to Directive 2001/29 and Article 2(3)(a) of Directive 2004/48, those rules laid down by the Member States may not affect the provisions of Directive 2000/31 and, more specifically, Articles 12 to 15 thereof.   
35      Consequently, those rules must, in particular, respect Article 15(1) of Directive 2000/31, which prohibits national authorities from adopting measures which would require an ISP to carry out general monitoring of the information that it transmits on its network.   
36      In that regard, the Court has already ruled that that prohibition applies in particular to national measures which would require an intermediary provider, such as an ISP, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights. Furthermore, such a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly (see   
L’Oréal and Others  
, paragraph 139).   
37      In those circumstances, it is necessary to examine whether the injunction at issue in the main proceedings, which would require the ISP to install the contested filtering system, would oblige it, as part of that system, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights.   
38      In that regard, it is common ground that implementation of that filtering system would require  
–        first, that the ISP identify, within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic;  
–        secondly, that it identify, within that traffic, the files containing works in respect of which holders of intellectual-property rights claim to hold rights;  
–        thirdly, that it determine which of those files are being shared unlawfully; and   
–        fourthly, that it block file sharing that it considers to be unlawful.   
39      Preventive monitoring of this kind would thus require active observation of all electronic communications conducted on the network of the ISP concerned and, consequently, would encompass all information to be transmitted and all customers using that network.   
40      In the light of the foregoing, it must be held that the injunction imposed on the ISP concerned requiring it to install the contested filtering system would oblige it to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the ISP to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31.   
41      In order to assess whether that injunction is consistent with European Union law, account must also be taken of the requirements that stem from the protection of the applicable fundamental rights, such as those mentioned by the referring court.   
42      In that regard, it should be recalled that the injunction at issue in the main proceedings pursues the aim of ensuring the protection of copyright, which is an intellectual-property right, which may be infringed by the nature and content of certain electronic communications conducted through the network of the ISP concerned.   
43      The protection of the right to intellectual property is indeed enshrined in Article 17(2) of the Charter of Fundamental Rights of the European Union (‘the Charter’). There is, however, nothing whatsoever in the wording of that provision or in the Court’s case-law to suggest that that right is inviolable and must for that reason be absolutely protected.   
44      As paragraphs 62 to 68 of the judgment in Case C-275/06   
Promusicae  
 [2008] ECR I-271 make clear, the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights.   
45      More specifically, it follows from paragraph 68 of that judgment that, in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures.   
46      Accordingly, in circumstances such as those in the main proceedings, national authorities and courts must, in particular, strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as ISPs pursuant to Article 16 of the Charter.  
47      In the present case, the injunction requiring the installation of the contested filtering system involves monitoring all the electronic communications made through the network of the ISP concerned in the interests of those rightholders. Moreover, that monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also future works that have not yet been created at the time when the system is introduced.   
48      Accordingly, such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly.   
49      In those circumstances, it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as ISPs.   
50      Moreover, the effects of that injunction would not be limited to the ISP concerned, as the contested filtering system may also infringe the fundamental rights of that ISP’s customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.   
51      It is common ground, first, that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users’ IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified.   
52      Secondly, that injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned.   
53      Consequently, it must be held that, in adopting the injunction requiring the ISP to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other.   
54      In the light of the foregoing, the answer to the questions submitted is that Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an ISP which requires it to install the contested filtering system.   
   
Costs  
55      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Directives:  
–          
2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’);  
–          
2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society;  
–          
2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights ;   
–          
95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and   
–          
2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),   
read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an internet service provider which requires it to install a system for filtering  
–          
all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;   
–          
which applies indiscriminately to all its customers;   
–          
as a preventive measure;   
–          
exclusively at its expense; and  
–          
for an unlimited period,   
which is capable of identifying on that provider’s network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual-property rights, with a view to blocking the transfer of files the sharing of which infringes copyright.

ID: c55fdefd-c1fd-4ede-b1cd-40f84076ad5c

Judgment of 24 Sep 2019, C-507/17 (  
Google  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right to erasure   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Territorial Scope   
   
JUDGMENT OF THE COURT (Grand Chamber)  
24 September 2019 (\*)  
(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Regulation (EU) 2016/679 — Internet search engines — Processing of data on web pages — Territorial scope of the right to de-referencing)  
In Case C-507/17,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Conseil d’État (Council of State, France), made by decision of 19 July 2017, received at the Court on 21 August 2017, in the proceedings  
Google LLC,  
 successor in law to Google Inc.,  
v  
Commission nationale de l’informatique et des libertés (CNIL),  
in the presence of:  
Wikimedia Foundation Inc.,  
Fondation pour la liberté de la presse,  
Microsoft Corp.,  
Reporters Committee for Freedom of the Press and Others,  
Article 19 and Others,  
Internet Freedom Foundation and Others,  
Défenseur des droits,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Arabadjiev, E. Regan, T. von Danwitz, C. Toader and F. Biltgen, Presidents of Chambers, M. Ilešič (Rapporteur), L. Bay Larsen, M. Safjan, D. Šváby, C.G. Fernlund, C. Vajda and S. Rodin, judges,  
Advocate General: M. Szpunar,  
Registrar: V. Giacobbo-Peyronnel, Administrator,  
having regard to the written procedure and further to the hearing on 11 September 2018,  
after considering the observations submitted on behalf of:  
–        Google LLC, by P. Spinosi, Y. Pelosi and W. Maxwell, avocats,  
–        the Commission nationale de l’informatique et des libertés (CNIL), by I. Falque-Pierrotin, J. Lessi and G. Le Grand, acting as Agents,  
–        Wikimedia Foundation Inc., by C. Rameix-Seguin, avocate,  
–        the Fondation pour la liberté de la presse, by T. Haas, avocat,  
–        Microsoft Corp., by E. Piwnica, avocat,  
–        the Reporters Committee for Freedom of the Press and Others, by F. Louis, avocat, and by H.-G. Kamann, C. Schwedler and M. Braun, Rechtsanwälte,  
–        Article 19 and Others, by G. Tapie, avocat, G. Facenna QC, and E. Metcalfe, Barrister,  
–        Internet Freedom Foundation and Others, by T. Haas, avocat,  
–        the Défenseur des droits, by J. Toubon, acting as Agent,  
–        the French Government, by D. Colas, R. Coesme, E. de Moustier and S. Ghiandoni, acting as Agents,  
–        Ireland, by M. Browne, G. Hodge, J. Quaney and A. Joyce, acting as Agents, and by M. Gray, Barrister-at-Law,  
–        the Greek Government, by E.-M. Mamouna, G. Papadaki, E. Zisi and S. Papaioannou, acting as Agents,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by R. Guizzi, avvocato dello Stato,  
–        the Austrian Government, by G. Eberhard and G. Kunnert, acting as Agents,  
–        the Polish Government, by B. Majczyna, M. Pawlicka and J. Sawicka, acting as Agents,  
–        the European Commission, by A. Buchet, H. Kranenborg and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 10 January 2019,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Google LLC, successor in law to Google Inc., and the Commission nationale de l’informatique et des libertés (French Data Protection Authority, France) (‘the CNIL’) concerning a penalty of EUR 100 000 imposed by the CNIL on Google because of that company’s refusal, when granting a de-referencing request, to apply it to all its search engine’s domain name extensions.  
   
Legal context  
   
European Union law  
   
Directive 95/46  
3        According to Article 1(1) thereof, the purpose of Directive 95/46 is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and to remove obstacles to the free movement of such data.  
4        Recitals 2, 7, 10, 18, 20 and 37 of Directive 95/46 state:  
‘(2)      Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;  
…   
(7)      Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level …   
…   
(10)      Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;  
…   
(18)      Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; …   
…   
(20)      Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;  
…   
(37)      Whereas the processing of personal data for purposes of journalism or for purposes of literary [or] artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing …’  
5        Article 2 of that directive provides:  
‘For the purposes of this Directive:  
(a)      “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); …   
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;  
…   
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; …   
…’  
6        Article 4 of that directive, entitled ‘National law applicable’, provides:  
‘1.      Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:  
(a)      the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;  
(b)      the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;  
(c)      the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.  
2.      In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.’  
7        Article 9 of Directive 95/46, entitled ‘Processing of personal data and freedom of expression’, states:  
‘Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.’  
8        Article 12 of that directive, entitled ‘Right of access’, provides:  
‘Member States shall guarantee every data subject the right to obtain from the controller:  
…   
(b)      as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
…’  
9        Article 14 of that directive, entitled ‘The data subject’s right to object’, provides:  
‘Member States shall grant the data subject the right:  
(a)      at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;  
…’  
10      Article 24 of Directive 95/46, entitled ‘Sanctions’, provides:  
‘The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.’  
11      Article 28 of that directive, entitled ‘Supervisory authority’, is worded as follows:  
‘1.      Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.  
…   
3.      Each authority shall in particular be endowed with:  
–        investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,  
–        effective powers of intervention, such as, for example, that of … ordering the blocking, erasure or destruction of data, [or] of imposing a temporary or definitive ban on processing …   
…   
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.  
4.      Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.  
…   
6.      Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.  
The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.  
…’  
   
Regulation (EU) 2016/679  
12      Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and Corrigendum OJ 2018 L 127, p. 2), which is based on Article 16 TFEU, is applicable, pursuant to Article 99(2) thereof, from 25 May 2018. Article 94(1) of that regulation provides that Directive 95/46 is repealed with effect from that date.  
13      Recitals 1, 4, 9 to 11, 13, 22 to 25 and 65 of that regulation state:  
‘(1)      The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (“the Charter”) and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.  
…   
(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, … the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information [and] freedom to conduct a business …   
…   
(9)       … Directive 95/46 … has not prevented fragmentation in the implementation of data protection across the Union … Differences in the level of protection … in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union …  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. …  
(11)      Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.  
…   
(13)      In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, … and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. …   
…   
(22)      Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. …  
(23)      In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. …  
(24)      The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.  
(25)      Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State’s diplomatic mission or consular post.  
…   
(65)      A data subject should have … a “right to be forgotten” where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject … However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information …’  
14      Article 3 of Regulation 2016/679, entitled ‘Territorial scope’, is worded as follows:  
‘1.      This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.  
2.      This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:  
(a)      the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or  
(b)      the monitoring of their behaviour as far as their behaviour takes place within the Union.  
3.      This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.’  
15      Article 4(23) of that regulation defines the concept of ‘cross-border processing’ as follows:  
‘(a)      processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or  
(b)      processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State’.  
16      Article 17 of that regulation, entitled ‘Right to erasure (“right to be forgotten”)’, is worded as follows:  
‘1.      The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:  
(a)      the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;  
(b)      the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;  
(c)      the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);  
(d)      the personal data have been unlawfully processed;  
(e)      the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;  
(f)      the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).  
…   
3.      Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:  
(a)      for exercising the right of freedom of expression and information;  
…’  
17      Article 21 of that regulation, entitled ‘Right to object’, provides, in paragraph 1 thereof:  
‘The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.’  
18      Article 55 of Regulation 2016/679, entitled ‘Competence’, which forms part of Chapter VI of that regulation, itself entitled ‘Independent supervisory authorities’, provides, in paragraph 1 thereof:  
‘Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.’  
19      Article 56 of that regulation, entitled ‘Competence of the lead supervisory authority’, states:  
‘1.      Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.  
2.      By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.  
3.      In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.  
4.      Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).  
5.      Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.  
6.      The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.’  
20      Article 58 of that regulation, entitled ‘Powers’, provides, in paragraph 2 thereof:  
‘Each supervisory authority shall have all of the following corrective powers:  
…   
(g)      to order the … erasure of personal data … pursuant to … [Article] … 17 …;  
…   
(i)      to impose an administrative fine … in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case’.  
21      Under Chapter VII of Regulation 2016/679, entitled ‘Cooperation and consistency’, Section I, entitled ‘Cooperation’, includes Articles 60 to 62 of that regulation. Article 60, entitled ‘Cooperation between the lead supervisory authority and the other supervisory authorities concerned’, provides:  
‘1.      The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.  
2.      The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.  
3.      The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.  
4.      Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.  
5.      Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.  
6.      Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.  
7.      The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.  
8.      By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.  
9.      Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. …  
10.      After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.  
11.      Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.  
…’  
22      Article 61 of that regulation, entitled ‘Mutual assistance’, states, in paragraph 1 thereof:  
‘Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.’  
23      Article 62 of that regulation, entitled ‘Joint operations of supervisory authorities’, provides:  
‘1.      The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.  
2.      Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. …’  
24      Section 2, entitled ‘Consistency’, of Chapter VII of Regulation 2016/679 includes Articles 63 to 67 of that regulation. Article 63, entitled ‘Consistency mechanism’, is worded as follows:  
‘In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.’  
25      Article 65 of that regulation, entitled ‘Dispute resolution by the Board’, provides, in paragraph 1 thereof:  
‘In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:  
(a)      where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;  
(b)      where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;  
…’  
26      Article 66 of that regulation, entitled ‘Urgency procedure’, provides, in paragraph 1 thereof:  
‘In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.’  
27      Article 85 of Regulation 2016/679, entitled ‘Processing and freedom of expression and information’, states:  
‘1.      Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.  
2.      For processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.  
…’  
   
French law  
28      Directive 95/46 is implemented in French law by loi n° 78-17, du 6 janvier 1978, relative à l’informatique, aux fichiers et aux libertés (Law No 78-17 of 6 January 1978 on information technology, data files and civil liberties), in the version applicable to the events in the main proceedings (‘the Law of 6 January 1978’).  
29      Article 45 of that law specifies that where the controller fails to fulfil the obligations laid down in that law, the President of the CNIL may serve notice on him to bring the established infringement to an end within a period which the President is to determine. If the controller does not comply with the formal notice served on him, the Select Panel of the CNIL may, after hearing both parties, impose, inter alia, a financial penalty.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
30      By decision of 21 May 2015, the President of the CNIL served formal notice on Google that, when granting a request from a natural person for links to web pages to be removed from the list of results displayed following a search conducted on the basis of that person’s name, it must apply that removal to all its search engine’s domain name extensions.  
31      Google refused to comply with that formal notice, confining itself to removing the links in question from only the results displayed following searches conducted from the domain names corresponding to the versions of its search engine in the Member States.  
32      The CNIL also regarded as insufficient Google’s further ‘geo-blocking’ proposal, made after expiry of the time limit laid down in the formal notice, whereby internet users would be prevented from accessing the results at issue from an IP (Internet Protocol) address deemed to be located in the State of residence of a data subject after conducting a search on the basis of that data subject’s name, no matter which version of the search engine they used.  
33      By an adjudication of 10 March 2016, the CNIL, after finding that Google had failed to comply with that formal notice within the prescribed period, imposed a penalty on that company of EUR 100 000, which was made public.  
34      By application lodged with the Conseil d’État (Council of State, France), Google seeks annulment of that adjudication.  
35      The Conseil d’État notes that the processing of personal data carried out by the search engine operated by Google falls within the scope of the Law of 6 January 1978, in view of the activities of promoting and selling advertising space carried on in France by its subsidiary Google France.  
36      The Conseil d’État also notes that the search engine operated by Google is broken down into different domain names by geographical extensions, in order to tailor the results displayed to the specificities, particularly the linguistic specificities, of the various States in which that company carries on its activities. Where the search is conducted from ‘google.com’, Google, in principle, automatically redirects that search to the domain name corresponding to the State from which that search is deemed to have been made, as identified by the internet user’s IP address. However, regardless of his or her location, the internet user remains free to conduct his or her searches using the search engine’s other domain names. Moreover, although the results may differ depending on the domain name from which the search is conducted on the search engine, it is common ground that the links displayed in response to a search derive from common databases and common indexing.  
37      The Conseil d’État considers that, having regard, first, to the fact that Google’s search engine domain names can all be accessed from French territory and, secondly, to the existence of gateways between those various domain names, as illustrated in particular by the automatic redirection mentioned above, as well as by the presence of cookies on extensions of that search engine other than the one on which they were initially deposited, that search engine, which, moreover, has been the subject of only one declaration to the CNIL, must be regarded as carrying out a single act of personal data processing for the purposes of applying the Law of 6 January 1978. As a result, the processing of personal data by the search engine operated by Google is carried out within the framework of one of its installations, Google France, established on French territory, and is therefore subject to the Law of 6 January 1978.  
38      Before the Conseil d’État, Google maintains that the penalty at issue is based on a misinterpretation of the provisions of the Law of 6 January 1978, which transpose Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, on the basis of which the Court, in its judgment of 13 May 2014,   
Google Spain and Google  
 (C-131/12, EU:C:2014:317), recognised a ‘right to de-referencing’. Google argues that this right does not necessarily require that the links at issue are to be removed, without geographical limitation, from all its search engine’s domain names. In addition, by adopting such an interpretation, the CNIL disregarded the principles of courtesy and non-interference recognised by public international law and disproportionately infringed the freedoms of expression, information, communication and the press guaranteed, in particular, by Article 11 of the Charter.  
39      Having noted that this line of argument raises several serious difficulties regarding the interpretation of Directive 95/46, the Conseil d’État has decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must the “right to de-referencing”, as established by the [Court] in its judgment of 13 May 2014, [  
Google Spain and Google  
 (C-131/12, EU:C:2014:317),] on the basis of the provisions of [Article 12(b) and subparagraph (a) of the first paragraph of Article 14] of Directive [95/46], be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester’s name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46]?  
(2)      In the event that Question 1 is answered in the negative, must the “right to de-referencing”, as established by the [Court] in the judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester’s name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States …?  
3.      Moreover, in addition to the obligation mentioned in Question 2, must the “right to de-referencing” as established by the [Court] in its judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the “geo-blocking” technique, from searches conducted on the basis of the requester’s name from an IP address deemed to be located in the State of residence of the person benefiting from the “right to de-referencing”, or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive [95/46], regardless of the domain name used by the internet user conducting the search?’  
   
Consideration of the questions referred  
40      The case in the main proceedings is the result of a dispute between Google and the CNIL as to how a search engine operator, where it establishes that a data subject is entitled to have one or more links to web pages containing personal data concerning him or her removed from the list of results which is displayed following a search conducted on the basis of his or her name, is to give effect to that right to de-referencing. Although Directive 95/46 was applicable on the date the request for a preliminary ruling was made, it was repealed with effect from 25 May 2018, from which date Regulation 2016/679 is applicable.  
41      The Court will examine the questions referred in the light of both that directive and that regulation in order to ensure that its answers will be of use to the referring court in any event.  
42      During the proceedings before the Court, Google explained that, following the bringing of the request for a preliminary ruling, it has implemented a new layout for the national versions of its search engine, in which the domain name entered by the internet user no longer determines the national version of the search engine accessed by that user. Thus, the internet user is now automatically directed to the national version of Google’s search engine that corresponds to the place from where he or she is presumed to be conducting the search, and the results of that search are displayed according to that place, which is determined by Google using a geo-location process.  
43      In those circumstances, the questions referred, which must be dealt with together, should be understood as seeking to ascertain, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679 are to be interpreted as meaning that, where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is required to carry out that de-referencing on all versions of its search engine, or whether, on the contrary, it is required to do so only on the versions of that search engine corresponding to all the Member States, or even only on the version corresponding to the Member State in which the request for de-referencing was made, using, where appropriate, the technique known as ‘geo-blocking’ in order to ensure that an internet user cannot, regardless of the national version of the search engine used, gain access to the links concerned by the de-referencing in the context of a search conducted from an IP address deemed to be located in the Member State of residence of the person benefiting from the right to de-referencing or, more broadly, in any Member State.  
44      As a preliminary point, it should be borne in mind that the Court has held that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 88).  
45      The Court has also stated that, when appraising the conditions for the application of those same provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him or her personally should, at that point in time, no longer be linked to his or her name by a list of results displayed following a search made on the basis of his or her name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his or her fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject’s name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his or her fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 99).  
46      In the context of Regulation 2016/679, that right of a data subject to de-referencing is now based on Article 17 of that regulation, which specifically governs the ‘right to erasure’, also referred to, in the heading of that article, as the ‘right to be forgotten’.  
47      Pursuant to Article 17(1) of Regulation 2016/679, a data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay where one of the grounds listed in that provision applies. Article 17(3) of that regulation specifies that Article 17(1) does not apply to the extent that processing is necessary for one of the reasons listed in the former provision. Those reasons include, in particular, under Article 17(3)(a) of that regulation, the exercise of the right of, inter alia, freedom of information of internet users.  
48      It follows from Article 4(1)(a) of Directive 95/46 and Article 3(1) of Regulation 2016/679 that both that directive and that regulation permit data subjects to assert their right to de-referencing against a search engine operator who has one or more establishments in the territory of the Union in the context of activities involving the processing of personal data concerning those data subjects, regardless of whether that processing takes place in the Union or not.  
49      In that regard, the Court has held that the processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that search engine and which orientates its activity towards the inhabitants of that Member State (judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 60).  
50      In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Union are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that search engine is, at the same time, the means enabling those activities to be performed, the display of the list of results being accompanied, on the same page, by the display of advertising linked to the search terms (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraphs 56 and 57).  
51      That being so, the fact that the search engine is operated by an undertaking that has its seat in a third State cannot result in the processing of personal data carried out for the purposes of the operation of that search engine in the context of the advertising and commercial activity of an establishment of the controller on the territory of a Member State escaping the obligations and guarantees laid down by Directive 95/46 and Regulation 2016/679 (see, to that effect, judgment of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 58).  
52      In the present case, it is apparent from the information provided in the order for reference, first, that Google’s establishment in French territory carries on, inter alia, commercial and advertising activities, which are inextricably linked to the processing of personal data carried out for the purposes of operating the search engine concerned, and, second, that that search engine must, in view of, inter alia, the existence of gateways between its various national versions, be regarded as carrying out a single act of personal data processing. The referring court considers that, in those circumstances, that act of processing is carried out within the framework of Google’s establishment in French territory. It thus appears that such a situation falls within the territorial scope of Directive 95/46 and Regulation 2016/679.  
53      By its questions, the referring court seeks to determine the territorial scope which must be conferred on a de-referencing in such a situation.  
54      In that regard, it is apparent from recital 10 of Directive 95/46 and recitals 10, 11 and 13 of Regulation 2016/679, which was adopted on the basis of Article 16 TFEU, that the objective of that directive and that regulation is to guarantee a high level of protection of personal data throughout the European Union.  
55      It is true that a de-referencing carried out on all the versions of a search engine would meet that objective in full.  
56      The internet is a global network without borders and search engines render the information and links contained in a list of results displayed following a search conducted on the basis of an individual’s name ubiquitous (see, to that effect, judgments of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 80, and of 17 October 2017,   
Bolagsupplysningen and Ilsjan  
, C-194/16, EU:C:2017:766, paragraph 48).  
57      In a globalised world, internet users’ access — including those outside the Union — to the referencing of a link referring to information regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself.  
58      Such considerations are such as to justify the existence of a competence on the part of the EU legislature to lay down the obligation, for a search engine operator, to carry out, when granting a request for de-referencing made by such a person, a de-referencing on all the versions of its search engine.  
59      That being said, it should be emphasised that numerous third States do not recognise the right to de-referencing or have a different approach to that right.  
60      Moreover, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality (see, to that effect, judgment of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48, and Opinion 1/15   
(EU-Canada PNR Agreement)  
 of 26 July 2017, EU:C:2017:592, point 136). Furthermore, the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world.  
61      While the EU legislature has, in Article 17(3)(a) of Regulation 2016/679, struck a balance between that right and that freedom so far as the Union is concerned (see, to that effect, today’s judgment,   
GC and Others   
(De-referencing of sensitive data)  
, C-136/17, paragraph 59), it must be found that, by contrast, it has not, to date, struck such a balance as regards the scope of a de-referencing outside the Union.  
62      In particular, it is in no way apparent from the wording of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 or Article 17 of Regulation 2016/679 that the EU legislature would, for the purposes of ensuring that the objective referred to in paragraph 54 above is met, have chosen to confer a scope on the rights enshrined in those provisions which would go beyond the territory of the Member States and that it would have intended to impose on an operator which, like Google, falls within the scope of that directive or that regulation a de-referencing obligation which also concerns the national versions of its search engine that do not correspond to the Member States.  
63      Moreover, although Regulation 2016/679 provides the supervisory authorities of the Member States, in Articles 56 and 60 to 66 thereof, with the instruments and mechanisms enabling them, where appropriate, to cooperate in order to come to a joint decision based on weighing a data subject’s right to privacy and the protection of personal data concerning him or her against the interest of the public in various Member States in having access to information, it must be found that EU law does not currently provide for such cooperation instruments and mechanisms as regards the scope of a de-referencing outside the Union.  
64      It follows that, currently, there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject, as the case may be, following an injunction from a supervisory or judicial authority of a Member State, to carry out such a de-referencing on all the versions of its search engine.  
65      Having regard to all of the foregoing, a search engine operator cannot be required, under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679, to carry out a de-referencing on all the versions of its search engine.  
66      Regarding the question whether such a de-referencing is to be carried out on the versions of the search engine corresponding to the Member States or only on the version of that search engine corresponding to the Member State of residence of the person benefiting from the de-referencing, it follows from, inter alia, the fact that the EU legislature has now chosen to lay down the rules concerning data protection by way of a regulation, which is directly applicable in all the Member States, which has been done, as is emphasised by recital 10 of Regulation 2016/679, in order to ensure a consistent and high level of protection throughout the European Union and to remove the obstacles to flows of personal data within the Union, that the de-referencing in question is, in principle, supposed to be carried out in respect of all the Member States.  
67      However, it should be pointed out that the interest of the public in accessing information may, even within the Union, vary from one Member State to another, meaning that the result of weighing up that interest, on the one hand, and a data subject’s rights to privacy and the protection of personal data, on the other, is not necessarily the same for all the Member States, especially since, under Article 9 of Directive 95/46 and Article 85 of Regulation 2016/679, it is for the Member States, in particular as regards processing undertaken solely for journalistic purposes or for the purpose of artistic or literary expression, to provide for the exemptions and derogations necessary to reconcile those rights with, inter alia, the freedom of information.  
68      It follows from, inter alia, Articles 56 and 60 of Regulation 2016/679 that, for cross-border processing as defined in Article 4(23) of that regulation, and subject to Article 56(2) thereof, the various national supervisory authorities concerned must cooperate, in accordance with the procedure laid down in those provisions, in order to reach a consensus and a single decision which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities in the context of all its establishments in the Union. Moreover, Article 61(1) of Regulation 2016/679 obliges the supervisory authorities, in particular, to provide each other with relevant information and mutual assistance in order to implement and to apply that regulation in a consistent manner throughout the Union, and Article 63 of that regulation specifies that it is for this purpose that provision has been made for the consistency mechanism set out in Articles 64 and 65 thereof. Lastly, the urgency procedure provided for in Article 66 of Regulation 2016/679 permits the immediate adoption, in exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, of provisional measures intended to produce legal effects on its own territory with a specified period of validity which is not to exceed three months.  
69      That regulatory framework thus provides the national supervisory authorities with the instruments and mechanisms necessary to reconcile a data subject’s rights to privacy and the protection of personal data with the interest of the whole public throughout the Member States in accessing the information in question and, accordingly, to be able to adopt, where appropriate, a de-referencing decision which covers all searches conducted from the territory of the Union on the basis of that data subject’s name.  
70      In addition, it is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject’s fundamental rights. Those measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject’s name (see, by analogy, judgments of 27 March 2014,   
UPC Telekabel Wien  
, C-314/12, EU:C:2014:192, paragraph 62, and of 15 September 2016,   
McFadden  
, C-484/14, EU:C:2016:689, paragraph 96).  
71      It is for the referring court to ascertain whether, also having regard to the recent changes made to its search engine as set out in paragraph 42 above, the measures adopted or proposed by Google meet those requirements.  
72      Lastly, it should be emphasised that, while, as noted in paragraph 64 above, EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights (see, to that effect, judgments of 26 February 2013,   
Åkerberg Fransson  
, C-617/10, EU:C:2013:105, paragraph 29, and of 26 February 2013,   
Melloni  
, C-399/11, EU:C:2013:107, paragraph 60), a data subject’s right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.  
73      In the light of all of the foregoing, the answer to the questions referred is that, on a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679, where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject’s name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.  
   
Costs  
74      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
On a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and of Article 17(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation), where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject’s name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.

ID: c9902594-6322-42a7-9321-8e39ffc94f36

of 26 Jan 2023, C-205/21 (  
Ministerstvo na vatreshnite raboti  
)  
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
Law Enforcement Directive   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Special categories of personal data   
Law Enforcement Directive   
Charter of fundamental rights of the EU   
 >   
Article 47 - Right to an effective remedy and to a fair trial   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Special categories of personal data   
Law Enforcement Directive   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Special categories of personal data   
   
JUDGMENT OF THE COURT (Fifth Chamber)  
26 January 2023 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Directive (EU) 2016/680 – Article 4(1)(a) to (c) – Principles relating to processing of personal data – Purpose limitation – Data minimisation – Article 6(a) – Clear distinction between personal data of different categories of data subjects – Article 8 – Lawfulness of processing – Article 10 – Transposition – Processing of biometric data and genetic data – Concept of ‘processing authorised by Member State law’ – Concept of ‘strictly necessary’ – Discretion – Charter of Fundamental Rights of the European Union – Articles 7, 8, 47, 48 and 52 – Right to effective judicial protection – Presumption of innocence – Limitation – Intentional criminal offence subject to public prosecution – Accused persons – Collection of photographic and dactyloscopic data in order for them to be entered in a record and taking of a biological sample for the purpose of creating a DNA profile – Procedure for enforcement of collection – Systematic nature of the collection)  
In Case C-205/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Spetsializiran nakazatelen sad (Specialised Criminal Court, Bulgaria), made by decision of 31 March 2021, received at the Court on 31 March 2021, in the criminal proceedings against  
V.S.,  
third party:  
Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost,  
THE COURT (Fifth Chamber),  
composed of E. Regan, President of the Chamber, D. Gratsias (Rapporteur), M. Ilešič, I. Jarukaitis and Z. Csehi, Judges,  
Advocate General: G. Pitruzzella,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        the Bulgarian Government, by M. Georgieva and T. Mitova, acting as Agents,  
–        the French Government, by R. Bénard, A.-L. Desjonquères, D. Dubois and T. Stéhelin, acting as Agents,  
–        the European Commission, by H. Kranenborg, M. Wasmeier and I. Zaloguin, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 30 June 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 4(1)(a) and (c), Article 6(a) and Articles 8 and 10 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89), and of Articles 3, 8, 48 and 52 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in criminal proceedings instituted against V.S., who, after being accused, refused to consent to collection by the police of her biometric and genetic data in order for them to be entered in a record.  
   
Legal context  
   
European Union law  
   
The GDPR  
3        Recital 19 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’), states:  
‘The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. …’  
4        Article 2 of the GDPR, headed ‘Material scope’, provides in paragraphs 1 and 2:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
…  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’  
5        Article 9 of the GDPR, headed ‘Processing of special categories of personal data’, provides in paragraphs 1, 2 and 4:  
‘1.      Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.  
2.      Paragraph 1 shall not apply if one of the following applies:  
(a)      the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, …  
(b)      processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law …  
(c)      processing is necessary to protect the vital interests of the data subject or of another natural person …  
(d)      processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim …  
(e)      processing relates to personal data which are manifestly made public by the data subject;  
(f)      processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;  
(g)      processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;  
(h)      processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services …  
(i)      processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;  
(j)      processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes …  
…  
4.      Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.’  
   
Directive 2016/680  
6        Recitals 9 to 12, 14, 26, 27, 31 and 37 of Directive 2016/680 state:  
‘(9)      … [the GDPR] lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union.  
(10)      In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.  
(11)      It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. …  
(12)      The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. … Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of [the GDPR].  
…  
(14)      Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the [EU Treaty] should not be considered to be activities falling within the scope of this Directive.  
…  
(26)      … The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. …  
(27)      For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.  
…  
(31)      It is inherent to the processing of personal data in the areas of judicial cooperation in criminal matters and police cooperation that personal data relating to different categories of data subjects are processed. Therefore, a clear distinction should, where applicable and as far as possible, be made between personal data of different categories of data subjects such as: suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses; persons possessing relevant information or contacts; and associates of suspects and convicted criminals. This should not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the [Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (the ECHR)], as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively.  
…  
(37)      Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. …’  
7        Article 1 of Directive 2016/680, headed ‘Subject matter and objectives’, provides in paragraphs 1 and 2:  
‘1.      This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.  
2.      In accordance with this Directive, Member States shall:  
(a)      protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; …  
(b)      ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.’  
8        Article 2 of Directive 2016/680, headed ‘Scope’, provides in paragraphs 1 and 3:  
‘1.      This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).  
…  
3.      This Directive does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
…’  
9        As set out in Article 3 of Directive 2016/680:  
‘For the purposes of this Directive:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “competent authority” means:  
(a)      any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; …  
…  
(12)      “genetic data” means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;  
(13)      “biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;  
…’  
10      Article 4 of Directive 2016/680, headed ‘Principles relating to processing of personal data’, provides in paragraph 1:  
‘Member States shall provide for personal data to be:  
(a)      processed lawfully and fairly;  
(b)      collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;  
(c)      adequate, relevant and not excessive in relation to the purposes for which they are processed;  
…’  
11      Article 6 of Directive 2016/680, headed ‘Distinction between different categories of data subject’, provides:  
‘Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:  
(a)      persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;  
(b)      persons convicted of a criminal offence;  
(c)      victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and  
(d)      other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).’  
12      Article 8 of Directive 2016/680, headed ‘Lawfulness of processing’, states:  
‘1.      Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.  
2.      Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.’  
13      Article 9 of Directive 2016/680, headed ‘Specific processing conditions’, provides in paragraphs 1 and 2:  
‘1.      Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, [the GDPR] shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.  
2.      Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), [the GDPR] shall apply to processing for such purposes …, unless the processing is carried out in an activity which falls outside the scope of Union law.’  
14      As set out in Article 10 of Directive 2016/680:  
‘Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:  
(a)      where authorised by Union or Member State law;  
(b)      to protect the vital interests of the data subject or of another natural person; or  
(c)      where such processing relates to data which are manifestly made public by the data subject.’  
15      Article 52 of Directive 2016/680, headed ‘Right to lodge a complaint with a supervisory authority’, states in paragraph 1:  
‘Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.’  
16      Article 53 of Directive 2016/680, headed ‘Right to an effective judicial remedy against a supervisory authority’, provides in paragraph 1:  
‘Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.’  
17      As set out in Article 54 of Directive 2016/680, headed ‘Right to an effective judicial remedy against a controller or processor’:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.’  
18      Article 63 of Directive 2016/680, headed ‘Transposition’, provides in paragraphs 1 and 4:  
‘1.      Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. …  
When Member States adopt those provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.  
…  
4.      Member States shall communicate to the [European] Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.’  
   
Bulgarian law  
   
The NK  
19      By virtue of Article 11(2) of the Nakazatelen kodeks (Criminal Code), in the version applicable to the main proceedings (‘the NK’), offences are intentional where the perpetrator is aware of the nature of his or her act or has intended or allowed the occurrence of the consequence of the offence. The vast majority of the offences provided for in the NK are intentional.  
20      Under Article 255 of the NK, ‘a person who evades the setting or payment of tax obligations of a significant amount’ in accordance with the detailed statutory rules expressly laid down is liable to a custodial sentence of one to six years and a fine of 2 000 leva (BGN) (approximately EUR 1000).  
21      Under Article 321(2) and (3) in conjunction with Article 94(20) of the NK, a person who participates in a criminal organisation formed with the aim of enrichment in order to commit offences punishable by a ‘custodial sentence’ exceeding 3 years is liable to a ‘custodial sentence’ of 3 to 10 years. It is also stated there that that is an intentional offence and that it is prosecuted under the ordinary law.  
   
The NPK  
22      Article 46(1) and Article 80 of the Nakazatelno-protsesualen kodeks (Code of Criminal Procedure), in the version applicable to the main proceedings (‘the NPK’), provide that criminal offences involve either public prosecution, that is to say, charges are brought by the prosecutor, or prosecution by the civil party. Almost all the offences under the NK involve public prosecution.  
23      Pursuant to Article 219(1) of the NPK, ‘where sufficient evidence that a particular person is guilty of a criminal offence subject to public prosecution is gathered’, that person is to be accused and informed thereof. He or she may be subject to various procedural coercive measures, while being able to defend himself or herself by providing explanation or adducing evidence.  
   
The ZZLD  
24      Under Article 51 of the zakon za zashtita na lichnite danni (Law on the protection of personal data) (DV No 1 of 4 January 2002; ‘the ZZLD’), the processing of genetic data and of biometric data for the purpose of uniquely identifying a natural person is to be allowed only where absolutely necessary and if the rights and freedoms of the data subject are appropriately safeguarded and the processing has been provided for by EU or Bulgarian law. If the processing is not provided for by EU or Bulgarian law, there must be vital interests allowing it or the data must have been made public by the data subject.  
   
The ZMVR  
25      Pursuant to Article 6 of the zakon sa Ministerstvo na vatreshnite raboti (Law on the Ministry of the Interior) (DV No 53 of 27 June 2014; ‘the ZMVR’), the Ministry of the Interior carries out a number of main activities, including operational research and surveillance activity, investigative activities relating to offences and intelligence activity.  
26      Pursuant to Article 18(1) of the ZMVR, the intelligence activity consists in gathering, processing, classifying, storing and using information. Pursuant to Article 20(1) thereof, the intelligence activity is based on information that is reproduced or is liable to be reproduced on recording media prepared by the authorities of the Ministry of the Interior.  
27      Article 25(1) of the ZMVR empowers the Ministry of the Interior to process personal data for the purpose of carrying out its activities. In view of Article 6 of the ZMVR, it follows that the Ministry of the Interior processes personal data in order to carry out its main activities, that is to say, its operational research activity, surveillance activity and investigative activity relating to offences.  
28      Article 25(3) of the ZMVR provides that the processing of personal data is to be carried out under that law, in accordance with the GDPR and the ZZLD.  
29      Under Article 25a(1) of the ZMVR, the processing of personal data involving genetic data and biometric data for the purpose of uniquely identifying a natural person is to be allowed only as provided for in Article 9 of the GDPR or Article 51 of the ZZLD.  
30      Under Article 27 of the ZMVR, data recorded by the police pursuant to Article 68 of that law are to be used only in connection with safeguarding national security, combating crime and maintaining law and order.  
31      Article 68 of the ZMVR is worded as follows:  
‘1.      The police authorities shall create a police record of persons who are accused of an intentional criminal offence subject to public prosecution. …  
2.      The creation of the police record is a form of processing of personal data of the persons referred to in paragraph 1, which shall be carried out in accordance with the requirements of this Law.  
3.      For the purposes of creating a police record, the police authorities shall:  
(1)      collect the personal data set out in Article 18 of the [zakon za balgaskite lichni dokumenti (Law on Bulgarian identity documents)];  
(2)      take a person’s fingerprints and photograph him or her;  
(3)      take samples to create a person’s DNA profile.  
4.      The consent of the person is not required to carry out the activities referred to in paragraph 3(1).  
5.      Persons shall be obliged to cooperate and not to hinder or obstruct the police authorities in carrying out the activities referred to in paragraph 3. In the event of a person’s refusal, the activities referred to in paragraph 3(2) and (3) shall be carried out by compulsion subject to authorisation from the judge of the court of first instance having jurisdiction over the offence subject to public prosecution of which the person has been accused.  
…’  
   
The NRISPR  
32      The naredba za reda za izvarshvane i snemane na politseyska registratsia (Regulation laying down detailed rules for the implementation of police records) (DV No 90 of 31 October 2014), in the version applicable to the main proceedings (‘the NRISPR’), which was adopted on the basis of Article 68(7) of the ZMVR, defines detailed rules for implementation of the police records provided for in Article 68 thereof.  
33      Pursuant to Article 2 of the NRISPR, the objectives of creating a police record are safeguarding national security, combating crime and maintaining law and order.  
34      Under Article 11(2) of the NRISPR, the person in respect of whom a police record must be created is to be given a declaration to be completed, in which he or she may express agreement or disagreement regarding the measures for the taking of photographs, fingerprints and DNA samples. Under Article 11(4) of the NRISPR, in the event of disagreement on the part of that person, the police are to submit an application to the court having jurisdiction in order for enforcement of those measures to be authorised.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
35      The Bulgarian authorities instituted criminal proceedings against two commercial companies for fraud concerning the setting and payment of tax obligations, on the basis of Article 255 of the NK.  
36      V.S. was accused by an order adopted on 1 March 2021, pursuant to Article 219 of the NPK, and served on her on 15 March 2021. She was accused, on the basis of Article 321(3)(2) of the NK, read in conjunction with Article 321(2) thereof, of participation with three other persons in a criminal organisation, formed with the aim of enrichment, with a view to committing offences under Article 255 of the NK in concert on Bulgarian territory.  
37      Following service of that order accusing her, V.S. was requested to cooperate in the creation of a police record. She completed a declaration form in which she stated that she had been informed of the existence of a statutory basis for the creation of the police record and that she refused to consent to the collection of the dactyloscopic and photographic data concerning her in order for them to be entered in the record and to the taking of a sample for the purpose of creating her DNA profile. The police did not collect the data and brought the matter before the referring court.  
38      The application by the police authorities to the referring court states that sufficient evidence of the guilt of the persons prosecuted in the criminal proceedings concerned, including of V.S., has been gathered. It is explained in the application that V.S. has been formally accused of an offence referred to in Article 321(3)(2) of the NK, read in conjunction with Article 321(2) thereof, and that she refused to consent to the collection of dactyloscopic and photographic data concerning her in order for them to be entered in the record and to the taking of a sample for the purpose of creating her DNA profile; the legal basis for the collection of those data is cited. Finally, the referring court is requested in the application to authorise enforcement of collection of the data. Only copies of the order accusing V.S. and of the declaration in which she refuses to give her consent to the creation of the police record were annexed to the application.  
39      The referring court has doubts as to whether the legislative and regulatory provisions of Bulgarian law that are applicable to the creation of a police record are compatible with EU law.  
40      In the first place, the referring court points out that Article 25(3) and Article 25a of the ZMVR refer to the GDPR and not to Directive 2016/680. It points out that, whilst the GDPR, by virtue of Article 2(2)(d) thereof, does not apply to the processing of personal data by competent bodies for the purposes of the prevention, investigation, detection or prosecution of criminal offences, Article 1(1) of Directive 2016/680 governs such processing. In addition, it observes that Article 9 of the GDPR expressly prohibits the processing of genetic and biometric data and that combating crime is not among the exceptions to that prohibition that are laid down in Article 9(2). Finally it adds that Article 51 of the ZZLD cannot by itself form the basis for the permissibility of processing of biometric and genetic data, as its permissibility must be provided for by EU or national law.  
41      In the light of those factors, the referring court wonders whether the view may be taken that, despite the reference to Article 9 of the GDPR, the processing of genetic and biometric data for purposes in the criminal field is permissible under national law, having regard to the fact that it is clearly authorised by Article 10 of Directive 2016/680, even though that directive is not referred to by the applicable provisions of the ZMVR.  
42      In the second place, if it should be held that Article 10 of Directive 2016/680 has been correctly transposed into national law or that there is a valid legal basis in national law for processing biometric and genetic data, the referring court is uncertain whether the requirement referred to in Article 10(a) of that directive, that such processing must be authorised by EU or Member State law, is satisfied where there is a contradiction between the applicable provisions of national law.  
43      The referring court takes the view that there is a contradiction between Article 25a of the ZMVR, which, by referring to Article 9 of the GDPR, appears not to authorise the collection of biometric and genetic data, and Article 68 of the ZMVR, which undoubtedly authorises it.  
44      In the third place, the referring court points out that, under Article 219(1) of the NPK, it is necessary to gather sufficient evidence that a particular person may be guilty in order for that person to be accused. It is unsure whether the criterion laid down in that provision corresponds to the criterion referred to in Article 6(a) of Directive 2016/680, which concerns persons with regard to whom there are ‘serious grounds for believing that they have committed [an] offence’. It is rather of the view that, in order to process biometric and genetic data, it is necessary to gather evidence that is more convincing than that which is required under the NPK in order to accuse a person, since the purpose of accusation is to inform that person of the grounds for suspecting him or her and of the possibility of defending himself or herself.  
45      In addition, the referring court states that Article 68 of the ZMVR does not provide that, in the context of the procedure for the mandatory creation of a police record, it must carry out any review as to the existence of serious grounds within the meaning of Article 6(a) of Directive 2016/680. On the contrary, under Article 68 of the ZMVR, it is sufficient for it to find that the person has been accused of an intentional offence subject to public prosecution. It thus has no jurisdiction to assess whether sufficient or solid evidence exists in support of such accusation, nor is it able, in practice, to carry out such an assessment since it has access not to the file but only to copies of the order accusing the person and of the declaration refusing consent to the collection of data by the police. Therefore, it is unsure whether, in those circumstances, the person who has refused to make available to the police the photographic, dactyloscopic and genetic data concerning him or her will enjoy effective judicial protection and observance of the right to be presumed innocent, guaranteed in Articles 47 and 48 of the Charter respectively.  
46      In the fourth place, the referring court infers from Article 4(1)(b) and (c), Article 8(1) and (2) and Article 10 of Directive 2016/680 that national law must confer on the competent authorities a certain degree of discretion when they collect biometric and genetic data by taking photographs, fingerprints and DNA samples. According to the referring court, that discretion should relate both to whether such collection must take place and to whether it must cover all the aforementioned categories of data. Finally, it takes the view that it must be inferred from the requirement, laid down in Article 10 of that directive, that the processing be ‘strictly necessary’ that the collection of such data can be authorised only where adequate reasons for its necessity are given.  
47      The referring court observes that the creation of a police record applies, however, mandatorily to all persons accused of intentional offences subject to public prosecution and to the three categories of personal data covered by that article, namely photographs, fingerprints and DNA samples.  
48      It observes, furthermore, that only the objectives of such processing of personal data are referred to by the ZMVR, namely the carrying out of investigative activity, including for the purpose of safeguarding national security, combating crime and maintaining law and order. On the other hand, national legislation does not require the specific necessity for the collection of biometric and genetic data to be established and it to be determined whether all of those data, or only a part thereof, suffice.  
49      The referring court is therefore uncertain whether the condition laid down by national law for authorising the creation of a police record, under which the person concerned must have been accused of an intentional offence subject to public prosecution, is sufficient to satisfy the requirements of Article 4(1)(a) and (c), Article 8(1) and (2) and Article 10 of Directive 2016/680.  
50      It was in those circumstances that the Spetsializiran nakazatelen sad (Specialised Criminal Court, Bulgaria) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 10 of Directive 2016/680 effectively transposed into national law – Article 25(3) and Article 25a of the [ZMVR] – by the inclusion of a reference to the similar provision in Article 9 of [the GDPR]?  
(2)      Is the requirement set in Article 10(a) of Directive 2016/680 in conjunction with Article 52 and with Articles 3 and 8 of the Charter, that any limitation on integrity and protection of personal data must be provided for by law, fulfilled if contradictory national provisions exist in relation to the permissibility of processing of genetic and biometric data for the purposes of creating a police record?  
(3)      Is a national law, namely Article 68(4) of the [ZMVR], which provides for the obligation of the court of first instance to order the forced collection of personal data (taking photographs for the file, taking fingerprints, and taking samples in order to create a DNA profile), compatible with Article 6(a) of Directive 2016/680 in conjunction with Article 48 of the Charter, if a person who is accused of an intentional criminal offence requiring public prosecution refuses to voluntarily cooperate in the collection of these personal data, without the court being able to assess whether there are serious grounds for believing that the person has committed the criminal offence of which he or she is accused?  
(4)      Is a national law, namely Article 68(1) to (3) of [the ZMVR], which provides, as a general rule, for the taking of photographs for the file, the taking of fingerprints, and the taking of samples in order to create a DNA profile for all persons who are accused of an intentional criminal offence requiring public prosecution compatible with Article 10, Article 4(1)(a) and (c), and Article 8(1) and (2) of Directive 2016/680?’  
51      By letter of 5 August 2022, the Sofiyski gradski sad (Sofia City Court, Bulgaria) informed the Court that, following a legislative amendment that entered into force on 27 July 2022, the Spetsializiran nakazatelen sad (Specialised Criminal Court) was dissolved and that certain criminal cases brought before it, including the case in the main proceedings, were transferred from that date to the Sofiyski gradski sad (Sofia City Court).  
   
Consideration of the questions referred  
   
The first and second  
 questions  
52      By its first and second questions, which it is appropriate to examine together, the referring court seeks, in essence, to ascertain whether Article 10(a) of Directive 2016/680, read in the light of Articles 3, 8 and 52 of the Charter, must be interpreted as meaning that the collection of biometric and genetic data by the police authorities with a view to their investigative activities for purposes of combating crime and maintaining law and order is authorised by Member State law, within the meaning of Article 10(a) of Directive 2016/680, where, first, the national provisions forming the legal basis for that authorisation refer to Article 9 of the GDPR, while reproducing the content of Article 10 of Directive 2016/680, and, second, those national provisions appear to lay down contradictory requirements so far as concerns the permissibility of such collection.  
   
Admissibility  
53      In its written observations, the Commission calls into question the admissibility of the first and second questions, submitting that the referring court, first, seeks solely to ascertain whether national law has in fact transposed Article 10 of Directive 2016/680, without expressing any doubts or raising any issues as to the precise meaning of that article, and second, does not state the reasons that prompted it to inquire about the interpretation or validity of the provisions of EU law at issue, in breach of Article 94 of the Rules of Procedure of the Court of Justice.  
54      In that regard, it should be recalled that, according to the Court’s settled case-law, it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions referred concern the interpretation or the validity of a rule of EU law, the Court is in principle bound to give a ruling. It follows that questions referred by national courts enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court only where it is apparent that the interpretation sought bears no relation to the actual facts of the main action or its object, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 20 October 2022, Digi, C-77/21, EU:C:2022:805, paragraph 17 and the case-law cited).  
55      To that end, in order to enable the Court to give an interpretation of EU law that is useful to the national court, the request for a preliminary ruling must, under Article 94(c) of the Rules of Procedure, contain a statement of the reasons which prompted the referring court to inquire about the interpretation or validity of certain provisions of EU law, and the relationship between those provisions and the national legislation applicable to the main proceedings (see, to that effect, judgment of 2 July 2015,   
Gullotta and Farmacia di Gullotta Davide & C.  
, C-497/12, EU:C:2015:436, paragraph 17 and the case-law cited).  
56      As regards the first and second questions, it is apparent from the order for reference that, in the case in the main proceedings, the referring court is uncertain whether the condition laid down in Article 10(a) of Directive 2016/680, under which processing of genetic and biometric data as covered by that article must be authorised by EU or Member State law, is satisfied so far as concerns the creation of a police record, which is at issue in that case.  
57      As the referring court states, in essence, in the request for a preliminary ruling, it is in that context that it seeks guidance from the Court regarding the interpretation of that condition. By its first question, it seeks to ascertain whether Article 10 of Directive 2016/680 may be regarded as having been correctly transposed by a provision of national law which refers only to Article 9 of the GDPR, but the content of which correspond to that of Article 10 of the directive. If the answer is in the affirmative, it also seeks to ascertain, by its second question, whether the collection of genetic and biometric data for the purpose of being entered in a record by the police may be regarded as being ‘authorised by Member State law’, within the meaning of Article 10(a) of the directive, that is to say, ‘provided for by law’, within the meaning of Article 52(1) of the Charter, where the provisions of national law which constitute the legal basis for that processing seem to lay down contradictory rules as to the permissibility of such processing.  
58      Consequently, the referring court identified clearly, in the request for a preliminary ruling, the applicable provisions of EU law, its queries concerning the interpretation of that law and the reasons which led it to submit the first and second questions to the Court. Furthermore, it is clear from that request that the interpretation of those provisions is connected to the object of the main proceedings, given that any finding by the referring court, in the light of the guidance provided by the Court of Justice, that the provisions of national law at issue do not satisfy the condition laid down in Article 10(a) of Directive 2016/680 is liable to result in the dismissal of the police authorities’ application before it seeking the compulsory collection of V.S.’s biometric and genetic data for the purpose of being entered in a record.  
59      It follows that the first and second questions are admissible.  
   
Substance  
60      As a preliminary point, it should be observed that, whilst the second question refers to Articles 3, 8 and 52 of the Charter, it is clear from the request for a preliminary ruling that the referring court’s queries relate only to whether the national legislation at issue in the main proceedings complies with the requirement, in Article 52(1), that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law. Consequently, the first and second questions must be examined in the light of only Article 52 of the Charter.  
61      First, it should be noted that, in the light of recital 19 of the GDPR and recitals 9 to 12 of Directive 2016/680 and by virtue of Article 2(1) and Article 9(1) and (2) of that directive, processing of personal data by a ‘competent authority’, within the meaning of Article 3(7) of that directive, may fall – depending on whether it is for the purposes, referred to in Article 1(1) thereof, of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, or for purposes other than those – either within the scope of the specific rules of that directive or within the scope of the general rules of that regulation, apart from where the exceptions to their respective scope, exhaustively listed in Article 2(3) of that directive and Article 2(2) of that regulation, apply.  
62      In particular, it should be noted that Article 9 of the GDPR and Article 10 of Directive 2016/680 both contain provisions governing the processing of special categories of personal data, which are regarded as sensitive data, including genetic and biometric data.  
63      In that regard, Article 10 of Directive 2016/680 provides that the processing of those sensitive data is to be allowed ‘only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject’ and only in three cases, including, by virtue of Article 10(a), where that processing is authorised by EU or Member State law. On the other hand, Article 9(1) of the GDPR lays down a general prohibition of the processing of those sensitive data, coupled with a list of situations, set out in Article 9(2), in which an exception to that prohibition may be made, a list which does not refer to any situation corresponding to that of data processing for purposes such as those specified in Article 1(1) of Directive 2016/680 and which would satisfy the requirement set out in Article 10(a) thereof. It follows that, whilst processing of biometric and genetic data by the competent authorities for purposes covered by Directive 2016/680 may be allowed provided that, in accordance with the requirements laid down in Article 10 thereof, it is strictly necessary, is subject to appropriate safeguards and is provided for by EU or Member State law, that will not necessarily be true of processing of such data that falls within the scope of the GDPR.  
64      Second, the scope of the requirement laid down in Article 10(a) of Directive 2016/680 that the processing of the personal data must have been ‘authorised by Union or Member State law’ must be determined in the light of the requirement enshrined in Article 52(1) of the Charter that any limitation on the exercise of a fundamental right must be ‘provided for by law’.  
65      In that regard, it is clear from the Court’s case-law that that requirement means that the legal basis authorising such a limitation must define the scope of that limitation sufficiently clearly and precisely (see, to that effect, judgment of 6 October 2020,   
État luxembourgeois (Right to bring an action against a request for information in tax matters)  
, C-245/19 and C-246/19, EU:C:2020:795, paragraph 76   
   
and the case-law cited  
)  
.  
66      Furthermore, it follows from the case-law recalled in the previous paragraph of the present judgment that there can be no uncertainty as to the provisions of EU law pursuant to which national law may authorise processing of biometric and genetic data, such as the processing at issue in the main proceedings, or as to the applicable conditions governing that authorisation. Data subjects and the courts having jurisdiction must be in a position to be able to determine precisely, in particular, the conditions under which that processing may take place and the purposes which it may lawfully pursue. However, the rules of the GDPR and those of the directive that are applicable to those requirements may differ.  
67      Accordingly, whilst the national legislature has the option to provide, in the same legislative instrument, for the processing of personal data for purposes covered by Directive 2016/680 and for other purposes covered by the GDPR, it has, on the other hand, the obligation, in accordance with the requirements set out in the previous paragraph of the present judgment, to make sure that there is no ambiguity as to the applicability of one or other of those two EU acts to the collection of biometric and genetic data.  
68      Third, as to the referring court’s queries regarding the possible incorrect transposition of Directive 2016/680, the provisions of national law transposing that directive, in particular Article 10, must be distinguished from those pursuant to which processing of data belonging to the special categories referred to in that article, inter alia biometric and genetic data, may be authorised, within the meaning of Article 10(a).  
69      Whilst, as is apparent from the second subparagraph of Article 63(1) thereof, Directive 2016/680 expressly requires the Member States to ensure that the necessary measures transposing the directive contain a reference to it or are accompanied by such a reference on the occasion of their official publication, which means, in any event, that a specific act transposing the directive must be adopted (see, to that effect, judgment of 25 February 2021,   
Commission   
v  
 Spain (Personal Data Directive – Criminal law)  
, C-658/19, EU:C:2021:138, paragraph 16 and the case-law cited), it does not require the measures of national law that authorise processing of data falling within its scope to contain such a reference. Thus, Article 63(4) of Directive 2016/680 merely provides that the Member States are to communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by the directive.  
70      Finally, it should be pointed out that, where a directive has been properly transposed, its effects reach individuals through the implementing measures adopted by the Member States concerned (see, to that effect, judgment of 15 May 1986,   
Johnston  
, 222/84, EU:C:1986:206, paragraph 51), unlike a regulation, the provisions of which generally have immediate effect in the national legal systems without it being necessary for the national authorities to adopt measures of application (see, to that effect, judgment of 7 April 2022,   
IFAP  
, C-447/20 and C-448/20, EU:C:2022:265, paragraph 88 and the case-law cited). It follows that, where the national legislature provides for the processing of biometric and genetic data by competent authorities, within the meaning of Article 3(7) of Directive 2016/680, which are capable of falling either within the scope of that directive or within the scope of the GDPR, it is open to it, for reasons of clarity and precision, to refer explicitly, on the one hand, to the provisions of national law transposing Article 10 of that directive and, on the other, to Article 9 of that regulation. However, that requirement of clarity and precision cannot demand, furthermore, that that directive be mentioned.  
71      Fourth, it should be noted that the obligation on a Member State, imposed by the third paragraph of Article 288 TFEU, to take all the measures necessary to achieve the result prescribed by a directive is binding on all the authorities of Member States including, for matters within their jurisdiction, the courts. It follows that, when national courts apply domestic law, they are bound to interpret it, so far as possible, in the light of the wording and the purpose of the relevant directive in order to achieve the result sought by the directive (see, to that effect, judgment of 7 November 2019,   
Profi Credit Polska  
, C-419/18 and C-483/18, EU:C:2019:930, paragraphs 73 and 75 and the case-law cited).  
72      Consequently, when faced with an apparent conflict, such as that described by it in the context of the second question, between, on the one hand, provisions of national legislation which seem to preclude the processing of genetic and biometric data by the competent authorities for purposes covered by Directive 2016/680 and, on the other hand, other provisions of that legislation which authorise such processing, the referring court is required to give those provisions an interpretation which safeguards that directive’s effectiveness. In particular, where it finds that provisions such as to satisfy the requirement referred to in Article 10(a) of the directive exist, it is for it to determine whether they do not in actual fact have a field of application different from that of the provisions with which they seem to conflict.  
73      In that regard, it should, in particular, be noted that Article 9(2) of Directive 2016/680 does not preclude the processing of biometric and genetic data by competent authorities, within the meaning of Article 3(7) of that directive, in connection with tasks other than those performed for the purposes set out in Article 1(1) of the directive. Also, as is apparent from paragraph 63 of the present judgment, Article 9 of the GDPR, which applies to the processing of such data, as long as the processing is not covered by the exceptions exhaustively listed in Article 2(2) thereof, does not prohibit such processing absolutely, provided that it corresponds to one of the situations set out in Article 9(2) of that regulation. That being so, it is for the referring court to determine whether the reference to the GDPR in those national provisions does not in actual fact relate to data processing by the competent authorities for purposes other than those covered by Directive 2016/680, with the result that those provisions do not conflict with the provisions which, in accordance with Article 10(a) of that directive, provide for the processing of such data for purposes which are covered by that directive.  
74      In the present instance, it is apparent from the order for reference that the provisions of national law giving rise to the questions submitted by the referring court are provisions of substantive law governing the activities of the Ministry of the Interior. The first of those provisions lays down that the processing of personal data by that ministry is to be carried out under the law in question, in accordance with the GDPR and the act of national law which transposes Directive 2016/680, and the second of those provisions states that the processing of personal data involving genetic data and biometric data for the purpose of uniquely identifying a natural person is to be allowed only as provided for in Article 9 of that regulation or in the provision of national law which transposes Article 10 of that directive. It is also apparent from the order for reference that the provision of substantive law which furnishes an express legal basis for the collection of biometric and genetic data, in the context of creation of a police record, pursues solely purposes of safeguarding national security, combating crime and maintaining law and order.  
75      Consequently, it is for the referring court to review whether the dual reference to Article 9 of the GDPR and to the provision of national law which transposes Article 10 of Directive 2016/680 may be justified by the fact that the scope of the provision of substantive law containing such a dual reference covers all the activities of the departments of the Ministry of the Interior, which, according to the information provided by the Bulgarian Government, include both the activities set out in Article 1(1) of that directive and other activities liable to fall within that regulation. Furthermore, it is for the referring court to satisfy itself that, in particular so far as concerns the provision of substantive law which furnishes a legal basis for the collection of biometric and genetic data in the context of creation of a police record, the set of relevant provisions of national law may be interpreted, in accordance with EU law, as making apparent, in a sufficiently clear, precise and unequivocal manner, in which cases the rules of national law transposing the directive at issue apply and in which cases it is the rules of the GDPR that are relevant.  
76      In the light of the foregoing, the answer to the first and second questions is that Article 10(a) of Directive 2016/680, read in the light of Article 52 of the Charter, must be interpreted as meaning that the processing of biometric and genetic data by the police authorities with a view to their investigative activities, for purposes of combating crime and maintaining law and order, is authorised by Member State law, within the meaning of Article 10(a) of Directive 2016/680, provided that the law of that Member State contains a sufficiently clear and precise legal basis to authorise that processing. The fact that the national legislative act containing such a legal basis refers, furthermore, to the GDPR, and not to Directive 2016/680, is not capable, in itself, of calling the existence of such authorisation into question, provided that it is apparent, in a sufficiently clear, precise and unequivocal manner, from the interpretation of the set of applicable provisions of national law that the processing of biometric and genetic data at issue falls within the scope of that directive, and not of that regulation.  
   
The third  
 question  
77      By its third question, the referring court asks, in essence, whether Article 6(a) of Directive 2016/680 and Articles 47 and 48 of the Charter must be interpreted as precluding national legislation which provides that, if the person accused of an intentional offence subject to public prosecution refuses to cooperate voluntarily in the collection of the biometric and genetic data concerning him or her in order for them to be entered in a record, the criminal court having jurisdiction must authorise enforcement of their collection, without having the power to assess whether there are serious grounds for believing that the person concerned has committed the offence of which he or she is accused.  
78      It should be noted at the outset that this question is asked by the referring court in relation to criminal proceedings in which a provision of national law is applicable that lays down that, if the person concerned refuses to cooperate in the collection of the biometric and genetic data concerning him or her in order for them to be entered in a record for purposes covered by Article 1(1) of Directive 2016/680, the court having jurisdiction to rule on that person’s criminal liability is empowered to authorise their collection. Furthermore, that provision of national law applies to the data concerning persons accused of intentional offences subject to public prosecution. According to the information provided by the referring court, the vast majority of the offences provided for by the NK are intentional and almost all involve public prosecution. Under the rules of Bulgarian criminal procedure, a person is accused when sufficient evidence that he or she is guilty of an offence subject to public prosecution is gathered.  
79      In addition, according to the explanation provided by the Bulgarian Government in the written answers to the questions asked by the Court, the rules relating to Bulgarian criminal procedure provide that accusation may occur at any time in the preliminary procedure – which constitutes the first stage of the criminal procedure, during which investigation is carried out and evidence is gathered – and, in any event, before the investigation is closed. As is apparent from the order for reference, and as the Bulgarian Government also explains, the person concerned may, after being so accused, present evidence in his or her defence, in particular in the course of the stage of disclosure of the investigative material, which takes place after closure of the investigation.  
80      However, the referring court states that the national legislation at issue does not confer on the court which authorises collection of the biometric and genetic data concerning the accused person in order for them to be entered in a record jurisdiction to assess the evidence on which that accusation is founded, a power which lies with the authorities handling the investigation. In addition, it explains that that court rules on the application for authorisation solely on the basis of a copy of the order accusing the person concerned and of the declaration by which he or she refuses to consent to the collection of those data.  
81      Against that background, the referring court’s third question should, as the Bulgarian Government and the Commission suggest, be regarded as divided into three parts. First, the referring court is uncertain whether Article 6(a) of Directive 2016/680, which refers to the category consisting of persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence, precludes national legislation which provides for the compulsory collection, in order to be entered in a record, of biometric and genetic data concerning a natural person in respect of whom sufficient evidence is gathered that he or she is guilty of an intentional offence subject to public prosecution, enabling, under national law, him or her to be accused. Second, it raises the question whether, having regard to the limits on the discretion of the court called upon to rule on the enforcement of such collection, that court is in a position to ensure the person concerned effective judicial protection, in accordance with Article 47 of the Charter. Third, it is uncertain whether, despite those limits, observance of the right to be presumed innocent which is referred to in Article 48 of the Charter can be ensured.  
   
The scope of Article 6(a) of Directive 2016/680  
82      Article 6 of Directive 2016/680 obliges the Member States to provide for the controller, ‘where applicable and as far as possible’, to make a clear distinction between personal data of different categories of data subjects, such as those referred to in Article 6(a) to (d), namely, respectively; persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; persons convicted of a criminal offence; victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and, finally, other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in Article 6(a) and (b).  
83      Thus, the Member States must ensure that a clear distinction is made between the data of the different categories of data subjects in such a way that, as the Advocate General has stated in point 27 of his Opinion, they are not subject without distinction – whatever the category to which they belong – to same degree of interference with their fundamental right to the protection of their personal data. In that regard, as may be inferred from recital 31 of Directive 2016/680, the category of persons defined in Article 6(a) of that directive corresponds to that of persons suspected of having committed a criminal offence.  
84      However, it follows from the wording of Article 6 of Directive 2016/680 that the obligation which that provision imposes on the Member States is not absolute. First, the phrase ‘where applicable and as far as possible’, which it contains, indicates that it is for the controller to determine, in each individual case, whether a clear distinction between the personal data of the different categories of data subjects may be made. Second, the words ‘such as’ which that article contains indicates that the categories of persons listed there are not exhaustive.  
85      Furthermore, the existence of sufficient items of evidence pointing to a person’s guilt constitutes, in principle, a serious ground for believing that he or she has committed the offence at issue. Thus, national legislation which provides for the compulsory collection of biometric and genetic data of natural persons in order for them to be entered in a record, where sufficient evidence is gathered that the person concerned is guilty of a criminal offence, appears consistent with the objective of Article 6(a) of Directive 2016/680.  
86      It follows from all the foregoing that Article 6(a) of Directive 2016/680 does not preclude national legislation which provides for the compulsory collection, in order to be entered in a record, of biometric and genetic data concerning persons in respect of whom sufficient evidence is gathered that they are guilty of an intentional offence subject to public prosecution and who have been accused for that reason.  
   
Observance of the right to effective judicial protection  
87      First, it should be noted that the right to effective judicial protection, enshrined in Article 47 of the Charter, must be accorded to any person relying on rights or freedoms guaranteed by EU law against a decision adversely affecting him or her which is such as to undermine those rights or freedoms (see, to that effect, judgment of 6 October 2020,   
État luxembourgeois (Right to bring an action against a request for information in tax matters)  
, C-245/19 and   
   
C  
-  
246  
/19, EU:C:2020:795,   
paragraphs 55  
, 57   
and  
 58   
and the case-law cited  
)  
.  
88      Consequently, any accused person who has opposed the collection of photographic, dactyloscopic and genetic data concerning him or her in the context of a procedure such as the creation of a police record, a procedure which has to comply with the requirements of Article 10 of Directive 2016/680, must, as Article 47 of the Charter requires, be able to enjoy the right to an effective remedy before a tribunal against the decision to authorise enforcement of their collection, for the purpose of relying on the rights which he or she derives from the safeguards laid down by that provision and, in particular, from the safeguard under Article 10(a) of the directive that collection of the biometric and genetic data must be carried out in compliance with the national legislation that authorises collection. In particular, that safeguard entails the court with jurisdiction having the ability to verify that the measure accusing the person concerned that constitutes the legal basis for the creation of the police record has been adopted – in accordance with the rules of national criminal procedure – in the light of sufficient evidence that he or she is guilty of an intentional offence subject to public prosecution.  
89      In that regard, it must be borne in mind that the right to effective judicial protection is not an absolute right and that, in accordance with Article 52(1) of the Charter, limitations may be placed upon it, on condition that (i) those limitations are provided for by law, (ii) they respect the essence of the rights and freedoms at issue, and (iii) in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (see, to that effect, judgment of 6 October 2020,   
État luxembourgeois (Right to bring an action against a request for information in tax matters)  
, C-245/19 and   
   
C  
-  
246  
/19, EU:C:2020:795,   
paragraphs 49  
 and  
 51   
and the case-law cited  
)  
.  
90      In addition, it should be noted that Article 54 of Directive 2016/680 imposes an obligation on the Member States to provide that a person who considers that his or her rights laid down in provisions adopted pursuant to that directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions has the right to an effective judicial remedy. It follows that the EU legislature did not itself limit the exercise of the right to an effective remedy enshrined in Article 47 of the Charter and that it is open to the Member States to limit its exercise, provided that they meet the requirements laid down in Article 52(1) of the Charter (see, to that effect, judgment of 6 October 2020,   
État luxembourgeois (Right to bring an action against a request for information in tax matters)  
, C-245/19 and C-246/19, EU:C:2020:795, paragraphs 63 and 64).  
91      Consequently, it should be determined whether, without prejudice to the judicial remedy provided for by national law pursuant to Article 54 of Directive 2016/680, the fact that the court having jurisdiction, with a view to authorising a measure enforcing the collection of biometric and genetic data concerning accused persons, cannot review, on the merits, the conditions for the accusation on which that enforcement measure is founded constitutes a permitted limitation of the right to effective judicial protection enshrined in Article 47 of the Charter.  
92      As regards the first condition referred to in paragraph 89 of the present judgment, in accordance with the case-law recalled in paragraph 65 of the present judgment, it is for the referring court to ascertain whether the limits placed on its discretion by national law, in the context of an application requesting it to authorise enforcement of the collection of biometric and genetic data concerning an accused person in order for them to be entered in a record, are laid down by national law sufficiently clearly and precisely.  
93      As regards the second condition, it follows from the case-law that the essence of the right to an effective remedy includes, among other aspects, the possibility, for the person who holds that right, of accessing a court or tribunal with the power to ensure respect for the rights guaranteed to that person by EU law and, to that end, to consider all the issues of fact and of law that are relevant for resolving the case before it (judgment of 6 October 2020,   
État luxembourgeois (Right to bring an action against a request for information in tax matters)  
, C-245/19 and   
   
C  
-  
246  
/19, EU:C:2020:795,   
paragraph 66   
   
and the case-law cited  
)  
.  
94      However, it also follows from the case-law of the Court that that condition does not mean, as such, that the holder of the right to effective judicial protection must have a direct remedy the primary object of which is to call into question a given measure, provided that one or more legal remedies also exist, before the various national courts having jurisdiction, enabling that rightholder to obtain, indirectly, judicial review of that measure ensuring respect for the rights and freedoms guaranteed to that rightholder by EU law (see, to that effect, judgment of 6 October 2020,   
État luxembourgeois (Right to bring an action against a request for information in tax matters)  
, C-245/19 and   
   
C  
-  
246  
/19, EU:C:2020:795,   
paragraph 79   
   
and the case-law cited  
)  
.  
95      In particular, as the Advocate General has noted, in essence, in point 36 of his Opinion, the third question is based on the hypothesis that the preliminary stage of the criminal procedure, during which enforcement of collection of the biometric and genetic data concerning an accused person in order for them to be entered in a record takes place, will be followed by a judicial stage. If the existence of sufficient items of incriminating evidence, a necessary condition in order for the person concerned to be capable of being compelled to consent to the collection of his or her biometric and genetic data, cannot be verified at the time of the application for authorisation of enforcement, it will necessarily have to be capable of being verified in that judicial stage, during which the court hearing the case must have the ability to consider all the relevant issues of fact and of law, in particular in order to verify whether those biometric and genetic data have been obtained in breach of the rights guaranteed by EU law to the person concerned (see, to that effect, judgment of 6 October 2020,   
État luxembourgeois (Right to bring an action against a request for information in tax matters)  
, C-245/19 and   
   
C  
-  
246  
/19, EU:C:2020:795,   
paragraphs 81   
   
to   
83   
and the case-law cited  
)  
.  
96      In any event, in accordance with Article 54 of Directive 2016/680, national law must provide the person concerned with the opportunity to effectively challenge the compulsory collection of his or her biometric and genetic data in judicial proceedings, founded on the alleged infringement, on account of collection of the data, of the rights conferred on him or her by that directive, without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority. Consequently, even if the preliminary stage of the criminal procedure is not followed by a judicial stage, in particular if there is no prosecution, the person concernedmust be able to obtain full judicial review of the legality of the processing of the data in question. Accordingly, where, in order to comply with the obligation in Article 54, national law provides such safeguards, a matter which is for the referring court to ascertain, respect for the essence of the right to effective judicial protection must be presumed, even if the court which authorises enforcement of the collection at issue does not itself have, at the time when it rules on it, the discretion necessary in order to grant such protection.  
97      As regards the third condition, it should be pointed out, first of all, that the collection of genetic and biometric data concerning persons accused in a criminal procedure, in order for them to be entered in a record, pursues purposes set out in Article 1(1) of Directive 2016/680, in particular those relating to the prevention, investigation, detection and prosecution of criminal offences, which constitute objectives of general interest recognised by the European Union.  
98      Such collection may contribute to the objective set out in recital 27 of Directive 2016/680, which states that, for the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.  
99      In the present instance, as the Bulgarian Government stated in its written observations and further explained in a written reply to a question asked by the Court, the creation of police records that is established by national law pursues two fundamental purposes. First, the data are gathered and processed in order to be compared with other data collected during investigations relating to other offences. That purpose, according to the Bulgarian Government, also concerns comparison with data collected in other Member States. Second, the data may also be processed for the purposes of the criminal procedure in which the person concerned has been accused.  
100    It may prove justified, during the preliminary stage of the criminal procedure, to shield temporarily from judicial review the assessment of the evidence on which accusation of the person concerned, and therefore the collection of his or her biometric and genetic data, is founded. Such review, at that stage, might impede the conduct of the criminal investigation in the course of which those data are being collected and excessively limit the investigators’ ability to clear up other offences on the basis of a comparison of those data with data gathered during other investigations. That limitation of effective judicial protection is therefore not disproportionate, provided that national law subsequently guarantees effective judicial review.  
101    It follows from all the foregoing that Article 47 of the Charter does not preclude a national court, when it rules on an application for authorisation of enforcement of the collection of biometric and genetic data of an accused person in order for them to be entered in a record, from being unable to assess the evidence on which the accusation of that person is based, provided that national law subsequently guarantees effective judicial review of the conditions for that accusation, from which the authorisation to collect those data arises.  
   
Observance of the presumption of innocence  
102    First of all, it should be noted that, under Article 48(1) of the Charter, the content of which corresponds to that of Article 6(2) of the Convention for the Protection of Human Rights and Fundamental Freedoms, everyone who has been charged is to be presumed innocent until proved guilty according to law.  
103    In particular, the Court has acknowledged that it follows from the case-law of the European Court of Human Rights inter alia that the presumption of innocence is infringed if a judicial decision concerning an accused person reflects the feeling that he or she is guilty, although his or her guilt has not previously been lawfully established (see, to that effect, judgment of 25 February 2021,   
Dalli  
 v   
Commission  
, C-615/19 P, EU:C:2021:133, paragraph 224 and the case-law cited).  
104    In addition, as is apparent from recital 31 of Directive 2016/680, the establishment of different categories of persons, the processing of whose personal data is to differ correspondingly, pursuant to Article 6 of that directive, should not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the Convention for the Protection of Human Rights and Fundamental Freedoms.  
105    As regards the referring court’s queries as to whether the right to be presumed innocent is observed by a judicial decision authorising the collection of biometric and genetic data concerning accused persons in order for them to be entered in a record, it must be stated, first, that, in so far as national law provides that their collection is limited to the category of persons who are accused, that is to say, a category of persons whose criminal liability has not yet been established, their collection cannot be regarded, in itself, as being such as to reflect the feeling of the authorities that those persons are guilty, within the meaning of the case-law cited in paragraph 103 of the present judgment.  
106    Second, where a judicial decision authorising the collection of biometric and genetic data concerning accused persons in order for them to be entered in a record merely takes note of the accusation of the person concerned and of his or her refusal to consent to such collection, it cannot be interpreted as defining a position on that person’s guilt or, therefore, as undermining the presumption that he or she is innocent.  
107    The fact that the court which must make such a judicial decision cannot assess, at that stage of the criminal procedure, whether the evidence on which the accusation of the person concerned is based is sufficient constitutes a guarantee for the latter of observance of the right to be presumed innocent.  
108    Such a guarantee is all the more necessary where national law, such as the provision at issue in the main proceedings, provides that the court having jurisdiction to rule on enforcement of collection of the biometric and genetic data concerning accused persons in order for them to be entered in a record is the court which, at the judicial stage of the criminal procedure, will have to rule on the criminal liability of such a person. Observance of the right to be presumed innocent requires that court to be free of any bias and any prejudice when it carries out that examination (see, to that effect, judgment of 16 November 2021,   
Prokuratura Rejonowa w Mińsku Mazowieckim and Others  
, C-748/19 to C-754/19, EU:C:2021:931, paragraph 88).  
109    It follows from the foregoing that the right to be presumed innocent, enshrined in Article 48 of the Charter, does not preclude accused persons, at the preliminary stage of the criminal procedure, from being the subject of a measure by which the biometric and genetic data concerning them are collected in order to be entered in a record and which is authorised by a court that does not have the power to assess, at that stage, the evidence upon which such accusation is based.  
110    It follows from all the foregoing that the answer to the third question is that Article 6(a) of Directive 2016/680 and Articles 47 and 48 of the Charter must be interpreted as not precluding national legislation which provides that, if the person accused of an intentional offence subject to public prosecution refuses to cooperate voluntarily in the collection of the biometric and genetic data concerning him or her in order for them to be entered in a record, the criminal court having jurisdiction must authorise a measure enforcing their collection, without having the power to assess whether there are serious grounds for believing that the person concerned has committed the offence of which he or she is accused, provided that national law subsequently guarantees effective judicial review of the conditions for that accusation, from which the authorisation to collect those data arises.  
   
The fo  
urth  
 question  
111    First of all, it should be recalled that, according to settled case-law, in the procedure laid down by Article 267 TFEU, providing for cooperation between national courts and the Court, it is for the latter to provide the national court with an answer which will be of use to it and enable it to determine the case before it. To that end, the Court may have to reformulate the questions referred to it (judgment of 15 July 2021,   
The Department for Communities in Northern Ireland  
, C-709/20, EU:C:2021:602, paragraph 61 and the case-law cited).  
112    As is clear from the order for reference and as has been observed in paragraphs 46 and 49 of the present judgment, in the context of the fourth question the referring court is uncertain as to the implications of the requirements set out in Article 4(1)(a) to (c), Article 8(1) and (2) and Article 10 of Directive 2016/680.  
113    Furthermore, as has been observed in paragraphs 46 to 48 of the present judgment, the referring court states that, although those provisions appear to it to require that the competent authorities have a discretion for the purpose of determining whether collection of biometric and genetic data is necessary and that they state adequate reasons for collecting them, the creation of a police record, as provided for by the legislation applicable in the main proceedings, applies mandatorily to all persons accused of intentional offences subject to public prosecution and to the three categories of biometric and genetic data covered by the provision of national law at issue in the main proceedings, without that legislation requiring the specific necessity to collect all those categories of data to be established.  
114    It follows that the fourth question should be understood as seeking to establish, in essence, whether Article 10 of Directive 2016/680, read in conjunction with Article 4(1)(a) to (c) and Article 8(1) and (2) thereof, must be interpreted as precluding national legislation which provides for the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution in order for them to be entered in a record, without laying down an obligation on the competent authority to determine and to demonstrate, first, that their collection is necessary for achieving the specific objectives pursued and, second, that those objectives cannot be achieved by collecting only a part of the data concerned.  
115    More specifically, the referring court’s queries concern the requirement set out in Article 10 of Directive 2016/680 that processing of the special categories of data referred to in that article is to be allowed ‘only where strictly necessary’.  
116    In that regard, in the first place, it should be noted that, as has been stated in paragraphs 62 and 63 of the present judgment, Article 10 of Directive 2016/680 constitutes a specific provision governing processing of the special categories of personal data, including biometric and genetic data. As is clear from the case-law, the purpose of that article is to ensure enhanced protection with regard to that processing, which, because of the particular sensitivity of the data at issue and the context in which they are processed, is liable, as is apparent from recital 37 of the directive, to create significant risks to fundamental rights and freedoms, such as the right to respect for private life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter (see, by analogy, judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 44).  
117    In the second place, as follows from the very terms in which it is set out in Article 10 of Directive 2016/680, the requirement that the processing of such data be allowed ‘only where strictly necessary’ [(‘  
uniquement en cas de nécessité absolue  
’ in the French-language version)] must be interpreted as establishing strengthened conditions for lawful processing of sensitive data, compared with those which follow from Article 4(1)(b) and (c) and Article 8(1) of that directive and refer only to the ‘necessity’ of data processing that falls generally, within the directive’s scope.  
118    Thus, first, the use of the adverb ‘only’ before the words ‘where strictly necessary’ underlines that the processing of special categories of data, within the meaning of Article 10 of Directive 2016/680, will be capable of being regarded as necessary solely in a limited number of cases. Second, the fact that the necessity for processing of such data is an ‘absolute’ one [(‘  
absolue  
’)] signifies that that necessity is to be assessed with particular rigour.  
119    The fact pleaded by the French Government that, in certain language versions of Article 10 of Directive 2016/680, that article refers to cases where the data processing is ‘strictly necessary’ is not decisive in that regard. That terminological variation does not alter the nature of the criterion thereby referred to and the requisite standard, since those language versions also establish a strengthened condition in order for the processing of sensitive data to be allowed, entailing a more rigorous assessment of its necessity than where the data processed do not fall within the scope of that article.  
120    Furthermore, as the Commission also notes, the requirement that processing of data falling within Article 10 of Directive 2016/680 is to be allowed only where strictly necessary did not appear in the proposal for a directive (COM(2012) 10 final) giving rise to that directive, but was introduced subsequently by the EU legislature, which thus clearly sought to impose a strengthened condition governing the necessity of data processing, in line with the objective pursued by that article of giving greater protection to persons in respect of the processing of sensitive data.  
121    In the third place, as regards what is entailed by the requirement that the processing of sensitive data is to be allowed ‘only where strictly necessary’, it should be pointed out that the specific requirements of Article 10 of Directive 2016/680 constitute a special form of implementation, applicable to certain categories of data, of the principles set out in Articles 4 and 8 of that directive, which must be observed by any data processing falling within the directive’s scope. Consequently, the scope of those various requirements must be determined in the light of those principles.  
122    In particular, first, the question whether collection of the biometric and genetic data of accused persons in order for them to be entered in a record is ‘strictly necessary’, within the meaning of Article 10 of Directive 2016/680, must be determined in the light of the purposes of their collection. In accordance with the purpose limitation principle set out in Article 4(1)(b) of that directive, those purposes must be ‘specified, explicit and legitimate’. Second, although the requirement that processing of the biometric and genetic data is to be allowed ‘only where strictly necessary’ corresponds, as has been observed in paragraphs 117 to 119 of the present judgment, to a requirement for enhanced protection of certain categories of data, it nonetheless constitutes a specific application to the categories of data referred to in Article 10 of the directive of the principle of data minimisation, set out in Article 4(1)(c) of the directive, under which personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.  
123    Furthermore, in the light of Article 4(1)(a) of Directive 2016/680, the scope of that requirement must also be determined having regard to Article 8(1) thereof, according to which Member States must provide, in particular, for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) of the directive, and to Article 8(2), which requires Member State law regulating processing within the scope of the directive to specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.  
124    In that regard, the purposes of processing biometric and genetic data cannot be indicated in terms that are too general, but have to be defined sufficiently precisely and specifically to enable assessment of whether that processing is ‘strictly necessary’.  
125    Furthermore, the requirement that processing of sensitive data be ‘strictly necessary’ entails particularly strict checking, in that context, as to whether the principle of data minimisation is observed.  
126    In that regard, first, it must be borne in mind, as is apparent from recital 26 of Directive 2016/680, that the requirement of necessity is met where the objective pursued by the data processing at issue cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 1 August 2022,   
Vyriausioji tarnybinės etikos komisija  
, C-184/20, EU:C:2022:601, paragraph 85 and the case-law cited). In particular, in the light of the enhanced protection of persons with regard to the processing of sensitive data, the controller in respect of that processing should satisfy itself that that objective cannot be met by having recourse to categories of data other than those listed in Article 10 of Directive 2016/680.  
127    Second, having regard to the significant risks posed by the processing of sensitive data to the rights and freedoms of data subjects, in particular in the context of the tasks of the competent authorities for the purposes set out in Article 1(1) of Directive 2016/680, the ‘strictly necessary’ requirement means that account is to be taken of the specific importance of the objective that such processing is intended to achieve. Such importance may be assessed, inter alia, on the basis of the very nature of the objective pursued – in particular of the fact that the processing serves a specific objective connected with the prevention of criminal offences or threats to public security displaying a certain degree of seriousness, the punishment of such offences or protection against such threats – and in the light of the specific circumstances in which that processing is carried out.  
128    In view of the foregoing, it must be held that national legislation which provides for the systematic collection of the biometric and genetic data of any person accused of an intentional offence subject to public prosecution is, in principle, contrary to the requirement laid down in Article 10 of Directive 2016/680 that processing of the special categories of data referred to in that article is to be allowed ‘only where strictly necessary’.  
129    Such legislation is liable to lead, in an indiscriminate and generalised manner, to collection of the biometric and genetic data of most accused persons since the concept of ‘intentional criminal offence subject to public prosecution’ is particularly general and is liable to apply to a large number of criminal offences, irrespective of their nature and gravity.  
130    It is true that such legislation restricts the scope of the collection of biometric and genetic data to persons accused at the investigation stage of a criminal procedure, that is to say, to persons with regard to whom there are serious grounds for believing that they have committed a criminal offence, within the meaning of Article 6(a) of Directive 2016/680. However, the mere fact that a person is accused of an intentional criminal offence subject to public prosecution cannot be regarded as a factor that in itself enables it to be presumed that the collection of his or her biometric and genetic data is strictly necessary in the light of the purposes that it pursues and given the resulting interference with fundamental rights, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.  
131    Thus, first, where there are serious grounds for believing that the person in issue has committed a criminal offence, justifying his or her being accused, a situation which presupposes that sufficient evidence of that person’s involvement in the offence has already been gathered, it is possible that the collection both of the biometric data and of the genetic data will not reflect any specific necessity for the purposes of the criminal procedure in progress.  
132    Second, the likelihood of the biometric and genetic data of an accused person being strictly necessary in connection with procedures other than the procedure in which that accusation has taken place can be determined only in the light of all the relevant factors, such as, in particular, the nature and gravity of the presumed offence of which he or she is accused, the particular circumstances of that offence, any link between that offence and other procedures in progress, and the criminal record or individual profile of the person in issue.  
133    That being so, it is for the referring court to verify whether, in order to ensure the effectiveness of Article 10 of Directive 2016/680, it is possible to interpret the national legislation providing for the enforcement in question in a manner consistent with EU law. In particular, it is for the referring court to verify whether national law enables it to be assessed whether it is ‘strictly necessary’ to collect both the biometric data and the genetic data of the data subject in order for them to be entered in a record. For that purpose, it should, inter alia, be possible to verify whether the nature and gravity of the offence of which the data subject in the main proceedings is suspected or whether other relevant factors, such as those referred to in paragraph 132 of the present judgment, may constitute circumstances capable of establishing that collection is ‘strictly necessary’. Furthermore, it should be checked whether the collection of civil status data, which is also provided for in the context of the creation of a police record, as the Bulgarian Government confirmed in a written reply to a question asked by the Court, does not in itself enable the objectives pursued to be met.  
134    If national law does not guarantee such review of the measure whereby biometric and genetic data are collected, it is for the referring court to ensure that Article 10 of Directive 2016/680 is given full effect by dismissing the police authorities’ application requesting it to authorise enforcement of their collection.  
135    It follows from all the foregoing that Article 10 of Directive 2016/680, read in conjunction with Article 4(1)(a) to (c) and Article 8(1) and (2) thereof, must be interpreted as precluding national legislation which provides for the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution in order for them to be entered in a record, without laying down an obligation on the competent authority to verify whether and demonstrate that, first, their collection is strictly necessary for achieving the specific objectives pursued and, second, those objectives cannot be achieved by measures constituting a less serious interference with the rights and freedoms of the person concerned.  
   
Costs  
136    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Fifth Chamber) hereby rules:  
1.        
Article 10(a) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, read in the light of Article 52 of the Charter of Fundamental Rights of the European Union,  
must be interpreted as meaning that the processing of biometric and genetic data by the police authorities with a view to their investigative activities, for purposes of combating crime and maintaining law and order, is authorised by Member State law, within the meaning of Article 10(a) of Directive 2016/680, provided that the law of that Member State contains a sufficiently clear and precise legal basis to authorise that processing. The fact that the national legislative act containing such a legal basis refers, furthermore, to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and not to Directive 2016/680, is not capable, in itself, of calling the existence of such authorisation into question, provided that it is apparent, in a sufficiently clear, precise and unequivocal manner, from the interpretation of the set of applicable provisions of national law that the processing of biometric and genetic data at issue falls within the scope of that directive, and not of that regulation.  
2.        
Article 6(a) of Directive 2016/680 and Articles 47 and 48 of the Charter of Fundamental Rights of the European Union  
must be interpreted as not precluding national legislation which provides that, if the person accused of an intentional offence subject to public prosecution refuses to cooperate voluntarily in the collection of the biometric and genetic data concerning him or her in order for them to be entered in a record, the criminal court having jurisdiction must authorise a measure enforcing their collection, without having the power to assess whether there are serious grounds for believing that the person concerned has committed the offence of which he or she is accused, provided that national law subsequently guarantees effective judicial review of the conditions for that accusation, from which the authorisation to collect those data arises.  
3.        
Article 10 of Directive 2016/680, read in conjunction with Article 4(1)(a) to (c) and Article 8(1) and (2) thereof,  
must be interpreted as precluding national legislation which provides for the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution in order for them to be entered in a record, without laying down an obligation on the competent authority to verify whether and demonstrate that, first, their collection is strictly necessary for achieving the specific objectives pursued and, second, those objectives cannot be achieved by measures constituting a less serious interference with the rights and freedoms of the person concerned.

ID: c9b5be88-39f3-4ba3-bcd8-ead5f1335e35

Judgment of 20 Sep 2022, C-793/19 (  
SpaceNet  
)  
E-privacy Directive   
 >   
Electronic communications   
 >   
Confidentiality of electronic communications   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Location data   
   
JUDGMENT OF THE COURT (Grand Chamber)  
20 September 2022 (\*)  
[Text rectified by order of 27 October 2022]  
(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Confidentiality of communications – Providers of electronic communications services – General and indiscriminate retention of traffic and location data – Directive 2002/58/EC – Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 6, 7, 8 and 11 and Article 52(1) – Article 4(2) TEU)  
In Joined Cases C-793/19 and C-794/19,  
REQUESTS for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Germany), made by decisions of 25 September 2019, received at the Court on 29 October 2019, in the proceedings  
Bundesrepublik Deutschland,  
 represented by the Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,  
v  
SpaceNet AG  
 (C-793/19),  
Telekom Deutschland GmbH  
 (C-794/19),  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis and I. Ziemele, Presidents of Chambers, T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (Rapporteur), N. Piçarra, L.S. Rossi and A. Kumin, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 13 September 2021,  
after considering the observations submitted on behalf of:  
–        the Bundesrepublik Deutschland, represented by the Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, by C. Mögelin, acting as Agent,  
–        [As rectified by order of 27 October 2022] SpaceNet AG, by M. Bäcker, Universitätsprofessor,  
–        Telekom Deutschland GmbH, by T. Mayen, Rechtsanwalt,  
–        the German Government, by J. Möller, F. Halibi, M. Hellmann, D. Klebs and E. Lankenau, acting as Agents,  
–        the Danish Government, by M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen and M. Søndahl Wolff, acting as Agents,  
–        the Estonian Government, by A. Kalbus and M. Kriisa, acting as Agents,  
–        Ireland, by A. Joyce and J. Quaney, acting as Agents, and by D. Fennelly, Barrister-at-Law, and P. Gallagher, Senior Counsel,  
–        the Spanish Government, by L. Aguilera Ruiz, acting as Agent,  
–        the French Government, by A. Daniel, D. Dubois, J. Illouz, E. de Moustier and T. Stéhelin, acting as Agents,  
–        the Cypriot Government, by I. Neophytou, acting as Agent,  
–        the Netherlands Government, by M.K. Bulterman, A. Hanje and C.S. Schillemans, acting as Agents,  
–        the Polish Government, by B. Majczyna, D. Lutostańska and J. Sawicka, acting as Agents,  
–        the Finnish Government, by A. Laine and M. Pere, acting as Agents,  
–        the Swedish Government, by H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson and H. Shev, acting as Agents,  
–        the European Commission, by G. Braun, S.L. Kalėda, H. Kranenborg, M. Wasmeier and F. Wilman, acting as Agents,  
–        the European Data Protection Supervisor, by A. Buchta, D. Nardi, N. Stolič and K. Ujazdowski, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 18 November 2021,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), read in the light of Articles 6 to 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’) and Article 4(2) TEU.  
2        The requests have been made in proceedings between the Bundesrepublik Deutschland (Federal Republic of Germany), represented by the Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Agency for Electricity, Gas, Telecommunications, Post and Rail Networks, Germany), on the one hand, and SpaceNet AG (Case C-793/19) and Telekom Deutschland GmbH (Case C-794/19), on the other, concerning the obligation imposed on those companies to retain traffic and location data relating to their customers’ telecommunications.  
   
Legal context  
   
European Union law  
   
Directive 95/46/EC  
3        Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), was repealed, with effect from 25 May 2018, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation) (OJ 2016 L 119, p. 1).  
4        Article 3(2) of Directive 95/46 provided:  
‘This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
   
Directive 2002/58  
5        Recitals 2, 6, 7 and 11 of Directive 2002/58 state:  
‘(2)      This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the [Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of [the Charter].  
…  
(6)      The internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the internet open new possibilities for users but also new risks for their personal data and privacy.  
(7)      In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.  
…  
(11)      Like [Directive 95/46], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the [Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the … Convention for the Protection of Human Rights and Fundamental Freedoms.’  
6        Article 1 of that directive, entitled ‘Scope and aim’, provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.  
2.      The provisions of this Directive particularise and complement [Directive 95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.  
3.      This Directive shall not apply to activities which fall outside the scope of [the TFEU], such as those covered by Titles V and VI of the [TEU], and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.’  
7        Under Article 2 of that directive, entitled ‘Definitions’:  
‘Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.  
The following definitions shall also apply:  
(a)      “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  
(c)      “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
…’  
8        Article 3 of Directive 2002/58, headed ‘Services concerned’, provides:  
‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.’  
9        Article 5 of the directive, headed ‘Confidentiality of the communications’, provides:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
…  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with [Directive 95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
10      Article 6 of Directive 2002/58, entitled ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
…’  
11      Article 9 of that directive, entitled ‘Location data other than traffic data’, provides, in paragraph 1 thereof:  
‘Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …’  
12      Article 15 of Directive 2002/58, entitled ‘Application of certain provisions of Directive [95/46]’, provides, in paragraph 1 thereof:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of [Directive 95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].’  
   
German law  
   
The TKG  
13      Paragraph 113a(1), first sentence, of the Telekommunikationsgesetz (Law on Telecommunications) of 22 June 2004 (BGB1. 2004 I, p. 1190), in the version applicable to the dispute in the main proceedings (‘the TKG’), is worded as follows:  
‘The obligations in respect of the retention, use and security of the traffic data defined in Paragraphs 113b to 113g apply to operators which provide publicly available telecommunications services to end users.’  
14      Under Paragraph 113b of the TKG:  
‘(1)      Operators to which Paragraph 113a(1) applies shall retain data in national territory as follows:  
1.      for 10 weeks in the case of the data referred to in subparagraphs 2 and 3;  
2.      for four weeks in the case of the location data referred to in subparagraph 4.  
(2)      Providers of publicly available telecommunications services shall retain:  
1.      the telephone number or other identifier of the calling and called parties as well as, in the case of call switching or forwarding, of every other line involved,  
2.      the date and time of the start and end of the communication, stating the time zone,  
3.      where different services can be used in the context of the telephone service, information on the service used;  
4.      and also, in the case of mobile telephony services,  
(a)      the International Mobile Subscriber Identity of the calling and called parties,  
(b)      the international identifier of the calling and called terminals,  
(c)      in the case of pre-paid services, the date and time of the initial activation of the service, stating the time zone;  
5.      and, in the case of internet telephony services, the IP (internet protocol) addresses of the calling and called parties and the allocated identification numbers.  
Subparagraph 1 above shall apply   
mutatis mutandis  
.  
1.      to SMS, multimedia messaging or similar services; in such cases, the information referred to in item 2 of subparagraph 1 shall be replaced by the time of despatch and receipt of the message;  
2.      to unanswered calls or calls that are unsuccessful due to intervention on the part of the network manager …  
(3)      Providers of publicly available internet access services shall retain:  
1.      the IP address allocated to the subscriber for the purposes of using the internet;  
2.      the clear identifier of the connection that provides access to the internet and the allocated network identification number;  
3.      the date and time of the start and end of internet use from the allocated IP address, stating the time zone.  
(4)      Where mobile telephony services are used, the designation of the cell sites used at the start of the communication by the caller and the recipient must be retained. In the case of mobile usage of publicly available internet access services, the designation of the cell sites used at the start of the internet connection must be retained. Any data that enable identification of the geographical location and the directions of maximum radiation of the antennas serving the cell site in question should also be retained.  
(5)      The content of the communication, data on internet sites visited and data from email services may not be retained pursuant to this provision.  
(6)      Data underlying the communications referred to in Paragraph 99(2) may not be retained pursuant to this provision. This applies,   
mutatis mutandis  
, to telephone communications originating from the entities referred to in Paragraph 99(2). The second to seventh sentences of Paragraph 99(2) apply   
mutatis mutandis  
.  
…’  
15      The communications mentioned in Paragraph 99(2) of the TKG, to which Paragraph 113b(6) of the TKG refers, are communications with persons, authorities and organisations of a social or religious nature which offer solely or essentially telephone assistance in psychological or social emergencies to callers who in principle remain anonymous and which are, along with their staff, subject to specific confidentiality obligations in that respect. The exemption laid down in the second and fourth sentences of Paragraph 99(2) of the TKG is conditional on the inclusion, upon request, of those call lines on a register drawn up by the Federal Agency for Electricity, Gas, Telecommunications, Post and Rail Networks, after the operators of those call lines have established the nature of the services provided by producing a certificate issued by an authority, entity, body or foundation governed by public law.  
16      Under Paragraph 113c(1) and (2) of the TKG:  
‘(1)      Data retained pursuant to Paragraph 113b may be:  
1.      disclosed to a law enforcement authority, where the authority so requests under a statutory provision which authorises it to collect the data referred to in Paragraph 113b for the purposes of prosecuting particularly serious criminal offences;  
2.      disclosed to a security authority of the   
Länder  
, where the authority so requests under a statutory provision which authorises it to collect the data referred to in Paragraph 113b for the purposes of preventing a specific risk to a person’s physical integrity, life or freedom or to the continued existence of the Federal State or a   
Land  
;  
…  
(2)      Data retained pursuant to Paragraph 113b may not be used by persons who are subject to the obligations established in Paragraph 113a(1) for purposes other than those provided for in subparagraph 1.’  
17      Article 113d of the TKG states:  
‘A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that the data retained pursuant to the retention obligation in Paragraph 113b(1) are protected by state-of-the-art technical and organisational measures against unauthorised access and use. These measures shall include, in particular:  
1.      use of a particularly secure encryption method;  
2.      storage in separate storage facilities that are separate from those designated for normal operational tasks;  
3.      storage that provides a high level of protection against cyber-attacks, in isolated data processing computer systems;  
4.      measures to ensure that access to the data processing facilities is restricted to persons who have been specially authorised by the party subject to the obligation; and  
5.      a requirement for at least two persons who have been specially authorised by the party subject to the obligation to be involved when the data are accessed.’  
18      Paragraph 113e of the TKG reads as follows:  
‘(1)      A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that all access, in particular the reading, copying, alteration, deletion and blocking of data retained pursuant to the retention obligation under Paragraph 113b(1), is logged for data protection control purposes. The following data must be logged:  
1.      the time of access;  
2.      the persons accessing the data;  
3.      the purpose and nature of the access.  
(2)      The log data may not be used for purposes other than data protection control.  
(3)      A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that the log data are deleted after one year.’  
19      In order to ensure a particularly high level of security and quality of data, the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways establishes, in accordance with Paragraph 113f(1) of the TKG, a set of requirements which, pursuant to Paragraph 113f(2) thereof, must be continuously assessed and adapted where appropriate. Paragraph 113g of the TKG requires that specific security measures be integrated into the security policy statement which must be presented by the party subject to the obligation.  
   
The StPO  
20      The first sentence of Paragraph 100g(2) of the Strafprozessordnung (Code of Criminal Procedure; ‘the StPO’) is worded as follows:  
‘Where there is prima facie evidence that someone has been the perpetrator of or an accessory to one of the particularly serious criminal offences referred to in the second sentence or, in those cases where an attempted offence is punishable, that someone has attempted to commit the offence in question and it is a particularly serious instance of the offence, the traffic data retained pursuant to Paragraph 113b of the [TKG] may be collected if the investigation of the facts or the determination of the whereabouts of the person under investigation would otherwise be significantly impeded or impracticable and the collection of the data is proportionate to the importance of the matter.’  
21      Paragraph 101a(1) of the StPO establishes that judicial authorisation is required for the collection of traffic data pursuant to Paragraph 100g thereof. Under Paragraph 101a(2) of the StPO, the grounds of the judicial decision must include essential considerations relating to the necessity and appropriateness of the measure in the particular case in question. Paragraph 101a(6) of the StPO lays down an obligation to inform the participants in the telecommunications concerned.  
   
The disputes in the main proceedings and the question referred for a preliminary ruling  
22      SpaceNet and Telekom Deutschland provide publicly available internet access services in Germany. The latter also provides publicly available telephone services in Germany.  
23      Those service providers brought proceedings before the Verwaltungsgericht Köln (Administrative Court, Cologne, Germany), challenging the obligation imposed on them by the combined provisions of Paragraph 113a(1) and Paragraph 113b of the TKG to retain traffic and location data relating to their customers’ telecommunications as from 1 July 2017.  
24      By judgments of 20 April 2018, the Verwaltungsgericht Köln (Administrative Court, Cologne) held that SpaceNet and Telekom Deutschland were not required to retain the traffic data relating to the telecommunications, referred to in Paragraph 113b(3) of the TKG, of the customers to whom they provide internet access and that Telekom Deutschland was also not required to retain the traffic data relating to the telecommunications, referred to in the first and second sentences of Paragraph 113b(2) of the TKG, of customers to whom it provides publicly available telephone services. That court considered, in the light of the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), that that retention obligation was contrary to EU law.  
25      The Federal Republic of Germany brought appeals on a point of law against those judgments before the Bundesverwaltungsgericht (Federal Administrative Court, Germany), the referring court.  
26      The referring court considers that the question whether the retention obligation imposed by the combined provisions of Paragraph 113a(1) and Paragraph 113b of the TKG is contrary to EU law depends on the interpretation of Directive 2002/58.  
27      In that respect, the referring court states that the Court has already established definitively, in the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), that rules governing the retention of traffic and location data and access to those data by national authorities fall, in principle, within the scope of Directive 2002/58.  
28      It also states that the retention obligation at issue in the main proceedings, since it limits the rights deriving from Article 5(1), Article 6(1) and Article 9(1) of Directive 2002/58, could be justified only on the basis of Article 15(1) of that directive.  
29      In that respect, it notes that it follows from the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.  
30      According to the referring court, like the national legislation at issue in the cases which gave rise to that judgment, the national legislation at issue in the main proceedings does not require any reason for the retention of the data or any link between the data retained and a criminal offence or a risk to public security. That national legislation requires the general retention, without a reason, and without any distinction in terms of personal, temporal or geographical factors, of the majority of the traffic data relating to telecommunications.  
31      The referring court considers, however, that it cannot be ruled out that the retention obligation at issue in the main proceedings may be justified under Article 15(1) of Directive 2002/58.  
32      In the first place, it notes that, contrary to the national legislation at issue in the cases that gave rise to the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), the national legislation at issue in the main proceedings does not require the retention of all telecommunications traffic data of all subscribers and users in relation to all means of electronic communications. Not only is the content of communications excluded from the retention obligation, but data relating to websites visited, the data from electronic mail services and the data underlying social or religious communications to or from certain lines cannot be retained, as is apparent from Paragraph 113b(5) and (6) of the TKG.  
33      In the second place, that court indicates that Paragraph 113b(1) of the TKG provides for a retention period of 4 weeks for location data and 10 weeks for traffic data, whereas Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 (OJ 2006 L 105, p. 54), on which the national legislation at issue in the cases that gave rise to the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), were based, provided for a retention period of between six months and two years.  
34      According to the referring court, although the exclusion of certain means of communication or certain categories of data and the limitation of the retention period are not sufficient to eliminate all risk of establishing a comprehensive profile of the persons concerned, that risk would be at least considerably reduced in the context of the implementation of the national legislation at issue in the main proceedings.  
35      In the third place, that legislation contains strict limitations as regards the protection of retained data and access thereto. Thus, first, it ensures the effective protection of retained data against the risks of abuse and against any unlawful access to those data. Secondly, the data retained can be used only for the purposes of fighting serious crime or for the prevention of a specific risk to a person’s physical integrity, life or freedom or to the continued existence of the Federal Republic or a   
Land  
.  
36      In the fourth place, the interpretation of Article 15(1) of Directive 2002/58 to the effect that any data retention without a reason is generally incompatible with EU law could conflict with the Member States’ obligation to act, arising from the right to security enshrined in Article 6 of the Charter.  
37      In the fifth place, the referring court considers that an interpretation of Article 15 of Directive 2002/58 as precluding the general retention of data would considerably restrict the discretion of the national legislature in an area concerning the prosecution of crimes and public security, which, in accordance with Article 4(2) TEU, remains the sole responsibility of each Member State.  
38      In the sixth place, the referring court considers that it is necessary to take into account the case-law of the European Court of Human Rights and notes that that court has held that Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (‘the ECHR’) does not preclude national provisions providing for the bulk interception of cross-border flows of data, in view of the threats currently facing many States and the technological tools which terrorists and criminals may now use in order to commit wrongdoings.  
39      In those circumstances, the Bundesverwaltungsgericht (Federal Administrative Court) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
‘In the light of Articles 7, 8 and 11 and Article 52(1) of the [Charter], on the one hand, and of Article 6 of the [Charter] and Article 4 [TEU], on the other hand, is Article 15 of Directive [2002/58] to be interpreted as precluding national legislation which obliges providers of publicly available electronic communications services to retain traffic and location data of end users of those services where:  
(1)      that obligation does not require a specific reason in terms of location, time or region,  
(2)      the following data are the subject of the retention obligation in the provision of publicly available telephone services – including the transmission of SMS, multimedia messages or similar messages and unanswered or unsuccessful calls:  
(a)      the telephone number or other identifier of the calling and called parties as well as, in the case of call switching or forwarding, of every other line involved,  
(b)      the date and time of the start and end of the call or – in the case of the transmission of a short message, multimedia message or similar message – the times of dispatch and receipt of the message, and an indication of the relevant time zone,  
(c)      information regarding the service used, if different services can be used in the context of the telephone service,  
(d)      and also, in the case of mobile telephone services  
(i)      the International Mobile Subscriber Identity of the calling and called parties,  
(ii)      the international identifier of the calling and called terminal equipment,  
(iii)      in the case of pre-paid services, the date and time of the initial activation of the service, and an indication of the relevant time zone,  
(iv)      the designations of the cells that were used by the calling and called parties at the beginning of the call,  
(e)      in the case of internet telephone services, the Internet Protocol addresses of the calling and the called parties and allocated user IDs,  
(3)      the following data are the subject of the retention obligation in the provision of publicly available internet access services:  
(a)      the Internet Protocol address allocated to the subscriber for internet use,  
(b)      a unique identifier of the connection via which the internet use takes place, as well as an allocated user ID,  
(c)      the date and time of the start and end of the internet use at the allocated Internet Protocol address, and an indication of the relevant time zone,  
(d)      in the case of mobile use, the designation of the cell used at the start of the internet connection,  
(4)      the following data must not be retained:  
(a)      the content of the communication,  
(b)      data regarding the internet pages accessed,  
(c)      data from electronic mail services,  
(d)      data underlying links to or from specific connections of persons, authorities and organisations in social or ecclesiastical spheres,  
(5)      the retention period is 4 weeks for location data, that is to say, the designation of the cell used, and 10 weeks for the other data,  
(6)      effective protection of retained data against risks of abuse and against any unlawful access to those data is ensured, and  
(7)      the retained data may be used only to prosecute particularly serious criminal offences and to prevent a specific threat to a person’s physical integrity, life or freedom or to the continued existence of the Federal Republic or of a   
Land  
, with the exception of the Internet Protocol address allocated to a subscriber for internet use, the use of which data is permissible in the context of the provision of inventory data information for the prosecution of any criminal offence, maintaining public order and security and carrying out the tasks of the intelligence services?’  
   
Procedure before the Court  
40      By decision of the President of the Court of 3 December 2019, Cases C-793/19 and C-794/19 were joined for the purposes of the written and oral parts of the procedure and the judgment.  
41      By decision of the President of the Court of 14 July 2020, the proceedings in Joined Cases C-793/19 and C-794/19 were stayed pursuant to Article 55(1)(b) of the Rules of Procedure of the Court of Justice, pending delivery of the judgment in   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18).  
42      On 6 October 2020, the Court delivered its judgment in   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and, on 8 October 2020, the President of the Court ordered the resumption of the proceedings in Joined Cases C-793/19 and C-794/19.  
43      The referring court, to which the Registry communicated that judgment, stated that it was maintaining its request for a preliminary ruling.  
44      In that respect, the referring court first of all noted that the retention obligation provided for by the legislation at issue in the main proceedings concerns a smaller amount of data and a shorter retention period than that provided for by the national legislation at issue in the cases that gave rise to the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791  
)  
. Those particular features reduce the possibility that the data retained could allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained.  
45      Next, it reiterated that the national legislation at issue in the main proceedings ensures the effective protection of retained data against the risks of abuse and unlawful access.  
46      Lastly, it indicated that uncertainties remain as regards the question of the compatibility with EU law of the retention of IP addresses, provided for by the national legislation at issue in the main proceedings, due to an inconsistency between paragraphs 155 and 168 of the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791  
)  
. Thus, according to the referring court, uncertainty arises from that judgment as to whether the Court requires, for the retention of IP addresses, a ground for retention linked to the objective of safeguarding national security, combating serious crime or preventing serious threats to public security, as seems to follow from paragraph 168 of that judgment, or whether the retention of IP addresses is permitted even in the absence of a specific ground, since only the use of the retained data is limited by those objectives, as paragraph 155 of that judgment suggests.  
   
Consideration of the question referred  
47      By its question, the referring court seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 6 to 8 and 11 and Article 52(l) of the Charter and Article 4(2) TEU, must be interpreted as meaning that it precludes a national legislative measure which, with certain exceptions, requires providers of publicly available electronic communications services – for the purposes set out in Article 15(1) of that directive, and inter alia for the purposes of prosecuting serious criminal offences or preventing a specific risk to national security – to retain, in a general and indiscriminate way, most of the traffic and location data of the end users of those services, laying down a retention period of several weeks and rules intended to ensure the effective protection of the retained data against the risks of abuse and against any unlawful access to those data.  
   
Applicability of Directive 2002/58  
48      As regards the argument of Ireland and the French, Netherlands, Polish and Swedish Governments that the national legislation at issue in the main proceedings does not fall within the scope of Directive 2002/58, since it was adopted, inter alia, in order to safeguard national security, it is sufficient to note that national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes, inter alia, of protecting national security and combating crime, such as the legislation at issue in the main proceedings, falls within the scope of Directive 2002/58 (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 104).  
   
Interpretation of Article 15(1) of Directive 2002/58  
   
The principles drawn from the Court’s case-law  
49      It is settled case-law that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 32 and the case-law cited).  
50      It is clear from the wording itself of Article 15(1) of Directive 2002/58 that the legislative measures that it authorises Member States to take, under the conditions that it lays down, may seek only ‘to restrict the scope’ of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of Directive 2002/58 (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 33).  
51      As regards the system established by that directive of which Article 15(1) forms part, it must be recalled that, pursuant to the first and second sentences of Article 5(1) of that directive, Member States are required to ensure, through their national legislation, the confidentiality of communications by means of a public communications network and publicly available electronic communications services, as well as of the related traffic data. In particular, they are required to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1) of the same directive (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 34).  
52      In that regard, the Court has already held that Article 5(1) of Directive 2002/58 enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires inter alia that, in principle, persons other than users be prohibited from storing, without those users’ consent, those communications and data (judgments of 6 October 2020,   
La Quadrature du Net and Others,  
 C-511/18, C-512/18 and C-520/18, EU:C:2020:791  
, paragraph 107,   
and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 35).  
53      That provision reflects the objective pursued by the EU legislature when adopting Directive 2002/58. It is apparent from the Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which gave rise to Directive 2002/58, that the EU legislature sought to ‘ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used’. As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of that directive is to protect users of electronic communications services from risks for their personal data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, as stated in recital 2 of the directive, the EU legislature’s intent is to ensure full respect for the rights set out in Articles 7 and 8 of the Charter, relating, respectively, to respect for private and family life and the protection of personal data (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 36 and the case-law cited).  
54      In adopting Directive 2002/58, the EU legislature gave concrete expression to those rights, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise (judgments of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 109, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 37).  
55      As regards the processing and storage by electronic communications service providers of subscribers’ and users’ traffic data, Article 6 of Directive 2002/58 provides, in paragraph 1, that those data must be erased or made anonymous, when they are no longer needed for the purpose of the transmission of a communication, and states, in paragraph 2, that the traffic data necessary for the purposes of subscriber billing and interconnection fees may only be processed up to the end of the period during which the bill may lawfully be challenged or payment pursued. As regards location data other than traffic data, Article 9(1) of that directive provides that those data may be processed only subject to certain conditions and after they have been made anonymous or the consent of the users or subscribers obtained.  
56      Therefore, Directive 2002/58 does not merely create a framework for access to such data through safeguards to prevent abuse, but also enshrines, in particular, the principle of the prohibition of their storage by third parties (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 39).  
57      In so far as Article 15(1) of Directive 2002/58 permits Member States to adopt legislative measures that ‘restrict the scope’ of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of that directive, such as those arising from the principles of confidentiality of communications and the prohibition on storing related data recalled in paragraph 52 above, that provision provides for an exception to the general rule provided for inter alia in Articles 5, 6 and 9 and must thus, in accordance with settled case-law, be the subject of a strict interpretation. That provision, therefore, cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of those data, laid down in Article 5 of that directive, to become the rule, if the latter provision is not to be rendered largely meaningless (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 40 and the case-law cited).  
58      As regards the objectives that are capable of justifying a limitation of the rights and obligations laid down, in particular, in Articles 5, 6 and 9 of Directive 2002/58, the Court has previously held that the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 41 and the case-law cited).  
59      Furthermore, it is clear from the third sentence in Article 15(1) of Directive 2002/58 that measures taken by the Member States must comply with the general principles of EU law, which include the principle of proportionality, and ensure respect for the fundamental rights guaranteed by the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making them available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, but also with Article 11 of the Charter, relating to the freedom of expression, which constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the European Union is founded (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraphs 42 and 43 and the case-law cited).  
60      It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, first, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing those data, and, secondly, an interference with the fundamental rights to the respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive, whether the persons concerned have been inconvenienced in any way on account of that interference, or, furthermore, whether the data retained will or will not be used subsequently (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 44 and the case-law cited).  
61      That conclusion is all the more justified since traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoy special protection under EU law. Taken as a whole, those data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, those data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 45 and the case-law cited).  
62      Therefore, first, the retention of traffic and location data for policing purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of electronic communications systems from exercising their freedom of expression, guaranteed in Article 11 of the Charter, effects that are all the more serious given the quantity and breadth of data retained. Secondly, in view of the significant quantity of traffic and location data that may be continuously retained under a general and indiscriminate retention measure, as well as the sensitive nature of the information that may be gleaned from those data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access (judgment of 5 April 2022,  
 Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 46 and the case-law cited).  
63      That being said, in so far as Article 15(1) of Directive 2002/58 allows Member States to introduce the derogations referred to in paragraph 51 to 54 above, that provision reflects the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. Thus, in order to interpret Article 15(1) of Directive 2002/58 in the light of the Charter, account must also be taken of the importance of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter and of the importance of the objectives of protecting national security and combating serious crime in contributing to the protection of the rights and freedoms of others (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 48 and the case-law cited).  
64      Thus as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, it should be borne in mind that positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life. Such obligations may also arise from Article 7, concerning the protection of an individual’s home and communications, and Articles 3 and 4, as regards the protection of an individual’s physical and mental integrity and the prohibition of torture and inhuman and degrading treatment (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 49 and the case-law cited).  
65      In view of those different positive obligations, it is therefore necessary to strike a balance between the various interests and rights at issue and to establish a legal framework which enables such a balance to be struck (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 50 and the case-law cited).  
66      In that context, it is clear from the wording itself of the first sentence of Article 15(1) of Directive 2002/58 that the Member States may adopt a measure derogating from the principle of confidentiality referred to in paragraph 52 above where such a measure is ‘necessary, appropriate and proportionate within a democratic society’, and recital 11 of the directive specifies, in that respect, that a measure of that nature must be ‘strictly’ proportionate to the intended purpose.  
67      In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 52 and the case-law cited).  
68      More specifically, it follows from the Court’s case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 53 and the case-law cited).  
69      In order to satisfy the requirement of proportionality, the national legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subjected to automated processing, in particular where there is a significant risk of unlawful access to those data. Those considerations apply especially where the protection of the particular category of personal data that are sensitive data is at stake (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 54 and the case-law cited).  
70      Thus, national legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 55 and the case-law cited).  
71      As regards the public interest objectives that may justify a measure taken pursuant to Article 15(1) of Directive 2002/58, it is clear from the Court’s case-law, in particular the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that, in accordance with the principle of proportionality, there is a hierarchy amongst those objectives according to their respective importance and that the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entails (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 56).  
72      Thus, as regards safeguarding national security, the importance of which exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, the Court held that that provision, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 58 and the case-law cited).  
73      As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, detecting and prosecuting criminal offences in general (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 59 and the case-law cited).  
74      As regards the objective of combating serious crime, the Court held that national legislation providing, for that purpose, for the general and indiscriminate retention of traffic and location data exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society. In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of those data is essential for the right to privacy. Thus, and also taking into account, first, the dissuasive effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the Charter, referred to in paragraph 62 above, which is liable to result from the retention of those data, and, secondly, the seriousness of the interference entailed by such retention, it is necessary, within a democratic society, that retention be the exception and not the rule, as provided for in the system established by Directive 2002/58, and that those data should not be retained systematically and continuously. That conclusion applies even having regard to the objectives of combating serious crime and preventing serious threats to public security and to the importance that must be attached to them (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 65 and the case-law cited).  
75      However, the Court specified that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that, for the purposes of combating serous crime and preventing serious threats to public security, provide for:  
–        the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;  
–        the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;  
–        the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and  
–        recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (quick freeze) of traffic and location data in the possession of those service providers,  
provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse (judgments of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 67).  
   
A measure providing for general and indiscriminate retention of the majority of traffic and location data for a period of several weeks  
76      It is in the light of those governing considerations that the characteristics of the national legislation at issue in the main proceedings, highlighted by the referring court, must be examined.  
77      In the first place, as regards the extent of the data retained, it is apparent from the order for reference that, in the context of the provision of telephone services, the retention obligation laid down by that legislation covers, inter alia, the data necessary to identify the source of a communication and its destination, the date and time of the start and end of the communication or – in the case of communication by SMS, multimedia message or similar message – the time of dispatch and receipt of the message and, in the case of mobile use, the designation of the cell sites used by the caller and the recipient at the start of the communication. In the context of the provision of internet access services, the retention obligation covers, inter alia, the IP address assigned to the subscriber, the date and time of the start and end of internet use from the assigned IP address and, in the case of mobile use, the designation of the cell sites used at the beginning of the internet connection. The data enabling the identification of the geographical location and the directions of maximum radiation of the antennas serving the cell site in question are also retained.  
78      Although the national legislation at issue in the main proceedings excludes the content of the communication and the data concerning the websites visited from the retention obligation and requires the retention of the cell site designation only at the beginning of the communication, that was also true, in essence, of the national legislation transposing Directive 2006/24 at issue in the cases that gave rise to the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791). Despite those limitations, the Court held in that judgment that the categories of data retained under that directive and those national rules could allow very precise conclusions to be drawn concerning the private life of the persons concerned, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them and, in particular, provide the means of establishing a profile of those persons.  
79      It must also be noted that, although the legislation at issue in the main proceedings does not cover the data concerning the websites visited, it nevertheless provides for the retention of IP addresses. Since IP addresses may be used, among other things, to track an internet user’s complete clickstream and, therefore, his or her entire online activity, those data enable a detailed profile of the user to be established. Thus, the retention and analysis of those IP addresses which is required for such tracking constitute a serious interference with the fundamental rights of the internet user enshrined in Articles 7 and 8 of the Charter (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 153).  
80      In addition, and as SpaceNet observed in its written observations, the data relating to electronic mail services, although not covered by the retention obligation laid down by the legislation at issue in the main proceedings, represent only a very small part of the data in question.  
81      Thus, as the Advocate General observed, in essence, in point 60 of his Opinion, the retention obligation laid down by the national legislation at issue in the main proceedings applies to a very broad set of traffic and location data which corresponds, in essence, to those which led to the settled case-law referred to in paragraph 78 above.  
82      In addition, in response to a question put to it at the hearing, the German Government stated that only 1 300 entities were listed on the register of persons, authorities or organisations of a social or religious nature whose electronic communications data are not retained under Paragraph 99(2) and Paragraph 113b(6) of the TKG, which clearly represents a small proportion of all users of telecommunications services in Germany whose data fall within the scope of the retention obligation laid down by the national legislation at issue in the main proceedings. The data of users who are subject to a duty of professional secrecy, such as lawyers, doctors and journalists, are thus retained.  
83      It is therefore apparent from the order for reference that the retention of traffic and location data provided for by that national legislation concerns practically the entire population without those persons being, even indirectly, in a situation liable to give rise to criminal prosecutions. Similarly, that legislation requires the general retention, without a reason, and without any distinction in terms of personal, temporal or geographical factors, of most traffic and location data, the scope of which corresponds, in essence, to that of the data retained in the cases which led to the case-law referred to in paragraph 78 above.  
84      Accordingly, in the light of the case-law cited in paragraph 75 above, a data retention obligation such as that at issue in the main proceedings cannot be regarded as a targeted retention of data, contrary to the submissions of the German Government.  
85      In the second place, as regards the data retention period, it follows from the second sentence of Article 15(1) of Directive 2002/58 that the length of the retention period provided for by a national measure imposing a general and indiscriminate retention obligation is indeed a relevant factor, amongst others, in determining whether EU law precludes such a measure, since that sentence requires that that period be ‘limited’.  
86      In the present case, it is true that those periods – which amount, according to Paragraph 113b(1) of the TKG, to 4 weeks for location data and to 10 weeks for other data – are significantly shorter that those provided for by the national legislation imposing a general and indiscriminate retention obligation examined by the Court in its judgments of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
 (C-140/20, EU:C:2022:258).  
87      However, as is apparent from the case-law cited in paragraph 61 above, the seriousness of the interference stems from the risk, particularly in view of their number and variety, that the data retained, taken as a whole, may enable very precise conclusions to be drawn concerning the private life of the person or persons whose data have been retained and, in particular, provide the means of establishing a profile of the person or persons concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.  
88      Accordingly, the retention of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses, is in any event serious regardless of the length of the retention period and the quantity or nature of the data retained, when that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned (see, as regards access to such data, judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 39).  
89      Even the retention of a limited quantity of traffic or location data or the retention of those data for a short period are liable to provide very precise information on the private life of a user of a means of electronic communication. Furthermore, the quantity of the data available and the very specific information on the private life of the person concerned that results from the data can be assessed only after the data have been consulted. However, the interference resulting from the retention of those data necessarily occurs before the data and the information resulting therefrom can be consulted. Thus, the assessment of the seriousness of the interference that the retention constitutes is necessarily carried out on the basis of the risk generally pertaining to the category of data retained for the private lives of the persons concerned, without it indeed mattering whether or not the resulting information relating to the person’s private life is in actual fact sensitive (see, to that effect, judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications),  
 C-746/18, EU:C:2021:152, paragraph 40).  
90      In the present case, as is apparent from paragraph 77 above and as was confirmed at the hearing, a set of traffic and location data retained for 10 weeks and 4 weeks respectively may allow very precise conclusions to be drawn concerning the private lives of the persons whose data are retained, such as habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them and, in particular, enable a profile of those persons to be established.  
91      In the third place, as regards the safeguards provided for by the national legislation at issue in the main proceedings, which are intended to protect the retained data against the risks of abuse and against any unlawful access, it must be emphasised that the retention of and access to those data each constitute, as is clear from the case-law recalled in paragraph 60 above, separate interferences with the fundamental rights guaranteed by Articles 7 and 11 of the Charter, requiring a separate justification pursuant to Article 52(1) of the Charter. It follows that national legislation ensuring full respect for the conditions established by the case-law interpreting Directive 2002/58 as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference, which results from the general retention of those data provided for under that national legislation, with the rights guaranteed by Articles 5 and 6 of that directive and by the fundamental rights to which those articles give specific effect (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 47).  
92      In the fourth and last place, as regards the European Commission’s argument that particularly serious crime could be treated in the same way as a threat to national security, the Court has already held that the objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 61 and the case-law cited).  
93      Unlike crime, even particularly serious crime, a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalised and indiscriminate measure of retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 62 and the case-law cited).  
94      Thus, crime, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. To treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 63).  
   
The measures providing for targeted retention, expedited retention or retention of IP addresses  
95      Several governments, including the French Government, submit that only general and indiscriminate retention enables the efficient achievement of the objectives pursued by the retention measures and the German Government has argued, in essence, that that conclusion is not undermined by the fact that the Member States may have recourse to the targeted retention and expedited retention measures referred to in paragraph 75 above.  
96      In that regard, it must be observed, in the first place, that the effectiveness of criminal proceedings generally depends not on a single means of investigation but on all the means of investigation available to the competent national authorities for those purposes (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 69).  
97      In the second place, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by the case-law recalled in paragraph 75 above, allows Member States to adopt, for the purposes of combating serious crime and preventing serious threats to public security, not only measures for targeted retention and expedited retention, but also measures providing for the general and indiscriminate retention, first, of data relating to the civil identity of users of electronic communications systems and, secondly, of IP addresses assigned to the source of a connection (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 70).  
98      In that respect, it is common ground that retention of data relating to the civil identity of users of electronic communications systems may contribute to the fight against serious crime to the extent that those data make it possible to identify persons who have used those means in the context of planning or committing an act constituting serious crime (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 71).  
99      Directive 2002/58 does not preclude, for the purposes of combating crime in general, the generalised retention of data relating to civil identity. In those circumstances, it must be stated that neither the directive nor any other EU law act precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser’s identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 72).  
100    In addition, it should be recalled that the generalised retention of IP addresses of the source of connection constitutes a serious interference in the fundamental rights enshrined in Articles 7 and 8 of the Charter as those IP addresses may allow precise conclusions to be drawn concerning the private life of the user of the means of electronic communication concerned and may be a deterrent to the exercise of freedom of expression guaranteed in Article 11 of the Charter. However, as regards such retention, the Court has held that in order to strike the necessary balance between the rights and interests at issue as required by the case-law referred to in paragraphs 65 to 68 above, it is necessary to take into account, in a case of an offence committed online and, in particular, in cases of the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1, and corrigendum OJ 2012 L 18, p. 7), the fact that the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 73).  
101    In those circumstances, while it is true that a legislative measure providing for the retention of the IP addresses of all natural persons who own terminal equipment permitting access to the internet would catch persons who at first sight have no connection, within the meaning of the case-law cited in paragraph 70 above, with the objectives pursued, and it is also true, in accordance with what has been stated in paragraph 54 above, that internet users are entitled to expect, under Articles 7 and 8 of the Charter, that their identity will not, in principle, be disclosed, a legislative measure providing for the general and indiscriminate retention of only IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of those data (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 155).  
102    In the light of the seriousness of the interference entailed by that retention with the fundamental rights enshrined in Articles 7 and 8 of the Charter, only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying that interference. Moreover, the retention period must not exceed what is strictly necessary in the light of the objective pursued. Finally, a measure of that nature must establish strict conditions and safeguards concerning the use of those data, particularly via tracking, with regard to communications made and activities carried out online by the persons concerned (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 156).  
103    Thus, contrary to the observations of the referring court, there is no tension between paragraphs 155 and 168 of the judgment of 6 October 2020,   
La Quadrature du Net and Others   
   
(C-511/18, C-512/18 and C-520/18, EU:C:2020:791). As the Advocate General observed, in essence, in points 81 and 82 of his Opinion, it is clear from that paragraph 155, read in conjunction with paragraph 156 and paragraph 168 of that judgment, that only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying the general retention of IP addresses assigned to the source of a connection, irrespective of whether the persons concerned are liable to have at least an indirect link to the objectives pursued.  
104    In the third place, as regards legislative measures providing for a targeted retention and an expedited retention of traffic and location data, some of the arguments put forward by the Member States against such measures show a narrower understanding of the scope of those measures than that set out in the case-law referred to in paragraph 75 above. While, as is recalled in paragraph 57 above, those retention measures are a derogation within the system established by Directive 2002/58, that directive, read in the light of the fundamental rights enshrined in Articles 7, 8 and 11 and Article 52(1) of the Charter, does not make the possibility of issuing an order requiring a targeted retention subject to the condition either that the places likely to be the location of a serious crime or the persons suspected of being involved in such an act must be known in advance. Likewise, that directive does not require that the order requiring an expedited retention be limited to suspects identified in advance of that order (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 75).  
105    As regards, first, targeted retention, the Court has held that Article 15(1) of Directive 2002/58 does not preclude national legislation based on objective evidence which makes it possible to target persons whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 76 and the case-law cited).  
106    The Court stated, in that regard, that, while the objective evidence may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective and non-discriminatory factors, as posing a threat to public or national security in the Member State concerned (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 77).  
107    Member States thus have, inter alia, the option of imposing retention measures targeting persons who, on the basis of such an identification, are the subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending. Where that identification is based on objective and non-discriminatory factors, defined in national law, targeted retention in respect of persons thus identified is justified (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 78).  
108    Secondly, a targeted measure for the retention of traffic and location data may, at the choice of the national legislature and in strict compliance with the principle of proportionality, also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to serious crime, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 79 and the case-law cited).  
109    It should be borne in mind that, according to that case-law, the competent national authorities may adopt, for areas referred to in the preceding paragraph, a targeted measure of retention using a geographic criterion, such as, inter alia, the average crime rate in a geographical area, without that authority necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime. Since a targeted retention using that criterion is likely to concern, depending on the serious criminal offences in question and the situation specific to the respective Member States, both the areas marked by a high incidence of serious crime and areas particularly vulnerable to the commission of those acts, it is, in principle, not likely moreover to give rise to discrimination, as the criterion drawn from the average rate of serious crime is, in itself, entirely unconnected with any potentially discriminatory factors (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 80).  
110    In addition and above all, a targeted measure of retention covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect traffic data and, in particular, location data of all persons using, at a specific time, a means of electronic communication in one of those places. Thus, such a targeted retention measure may allow those authorities to obtain, through access to the retained data, information as to the presence of those persons in the places or geographical areas covered by that measure as well as their movements between or within those areas and to draw, for the purposes of combating serious crime, conclusions as to their presence and activity in those places or geographical areas at a specific time during the period of retention (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 81).  
111    It should also be noted that the geographic areas covered by such a targeted retention measure may and, where appropriate, must be amended in accordance with changes in the circumstances that justified their selection, thus making it possible to react to developments in the fight against serious crime. The Court has held that the duration of those targeted retention measures described in paragraphs 105 to 110 above must not exceed what is strictly necessary in the light of the objective pursued and the circumstances justifying them, without prejudice to the possibility of extending those measures should such retention continue to be necessary (judgments of 6 October 2020,   
La Quadrature du Net and Others,  
 C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 151, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 82).  
112    As regards the possibility of providing distinctive criteria other than a personal or geographic criterion for the targeted retention of traffic and location data, it is possible that other objective and non-discriminatory criteria may be considered in order to ensure that the scope of a targeted retention measure is as limited as is strictly necessary and to establish a connection, at least indirectly, between serious criminal acts and the persons whose data are retained. However, since Article 15(1) of Directive 2002/58 refers to legislative measures of the Member States, it is for the latter and not for the Court to identify those criteria, it being understood that there can be no question of reinstating, by that means, the general and indiscriminate retention of traffic and location data (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 83).  
113    In any event, as the Advocate General observed in point 50 of his Opinion, the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general and indiscriminate retention of traffic and location data (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 84).  
114    As regards, secondly, the expedited retention of traffic and location data processed and stored by providers of electronic communications services on the basis of Articles 5, 6 and 9 of Directive 2002/58 or on the basis of legislative measures taken under Article 15(1) of that directive, it should be noted that those data must, in principle, be erased or made anonymous, depending on the circumstances, at the end of the statutory periods within which those data must be processed and stored in accordance with the national provisions transposing that directive. Nevertheless, the Court has held that during that processing and storage, situations may arise in which it becomes necessary to retain those data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may reasonably be suspected (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 85).  
115    In such a situation, in the light of the balance that must be struck between the rights and interests at issue referred to in paragraphs 65 to 68 above, it is permissible for Member States to provide, in legislation adopted pursuant to Article 15(1) of Directive 2002/58, for the possibility of instructing, by means of a decision of the competent authority subject to effective judicial review, providers of electronic communications services to undertake the expedited retention of traffic and location data at their disposal for a specified period of time (judgments of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 163, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 86).  
116    To the extent that the purpose of that expedited retention no longer corresponds to the purpose for which those data were initially collected and retained and since any processing of data must, under Article 8(2) of the Charter, be consistent with specified purposes, Member States must make clear, in their legislation, for what purpose the expedited retention of data may occur. In the light of the serious nature of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter which such retention may entail, only actions to combat serious crime and, a fortiori, to safeguard national security are such as to justify such interference, on the condition that the measure and access to the retained data comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020,   
La Quadrature du Net and Others   
(C-511/18, C-512/18 and C-520/18, EU:C:2020:791) (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 87).  
117    The Court has stated that a measure of retention of that nature need not be limited to the data of persons who have been identified previously as being a threat to public security or national security of the Member State concerned or of persons specifically suspected of having committed a serious criminal offence or acts adversely affecting national security. According to the Court, while it must comply with the framework established by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, and taking into account the considerations set out in paragraph 70 above, such a measure may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that those data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, and his or her social or professional circle (judgments of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 165, and of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 88).  
118    Thus, a legislative measure may authorise the issuing of an instruction to providers of electronic communications services to carry out the expedited retention of traffic and location data, inter alia, of persons with whom, prior to the serious threat to public security arising or a serious crime being committed, a victim was in contact via those electronic means of communications (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 89).  
119    Such expedited retention may, according to the Court’s case-law recalled in paragraph 117 above and under the same conditions as those referred to in that paragraph, also be extended to specific geographic areas, such as the places of the commission of or preparation for the offence or attack on national security in question. It should be stated that the subject matter of such a measure may also be the traffic and location data relating to a place where a person, possibly the victim of a serious crime, has disappeared, on condition that that measure and access to the data so retained comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791) (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 90).  
120    Furthermore, it must be stated that Article 15(1) of Directive 2002/58 does not preclude the competent national authorities from ordering a measure of expedited retention at the first stage of an investigation into a serious threat to public security or a possible serious crime, namely from the time when those authorities may, in accordance with the relevant provisions of national law, commence such an investigation (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 91).  
121    Again as regards the variety of measures for the retention of traffic and location data referred to in paragraph 75 above, it must be stated that those various measures may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently. Accordingly, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by case-law resulting from the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), does not preclude a combination of those measures (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 92).  
122    In the fourth and final place, it must be emphasised that the proportionality of the measures adopted pursuant to Article 15(1) of Directive 2002/58 requires, according to the Court’s settled case-law, as recalled in the judgment of 6 October 2020,   
La Quadrature du Net and Others   
   
(C-511/18, C-512/18 and C-520/18, EU:C:2020:791), compliance not only with the requirements of aptitude and of necessity but also with that of the proportionate nature of those measures in relation to the objective pursued   
   
(judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 93).  
123    In that context, it should be recalled that, in paragraph 51 of its judgment of 8 April 2014,   
Digital Rights Ireland and Others  
 (C-293/12 and C-594/12, EU:C:2014:238), the Court held that while the fight against serious crime is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques, that objective of general interest, however fundamental it may be, does not, in itself, justify that a measure providing for the general and indiscriminate retention of all traffic and location data, such as that established by Directive 2006/24, should be considered to be necessary (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 94).  
124    In the same vein, the Court stated, in paragraph 145 of the judgment of 6 October 2020,   
La Quadrature du Net and Others   
(  
C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that even the positive obligations of the Member States which may arise, depending on the circumstances, from Articles 3, 4 and 7 of the Charter and which relate, as pointed out in paragraph 64 above, to the establishment of rules to facilitate effective action to combat criminal offences, cannot have the effect of justifying interference that is as serious as that entailed by national legislation providing for the retention of traffic and location data with the fundamental rights, enshrined in Articles 7 and 8 of the Charter, of practically the entire population, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 95).  
125    Furthermore, the judgments of the European Court of Human Rights of 25 May 2021,   
Big Brother Watch and Others v. the United Kingdom  
 (CE:ECHR:2021:0525JUD005817013), and of 25 May 2021,   
Centrum för Rättvisa v. Sweden  
 (CE:ECHR:2021:0525JUD003525208), relied on by certain governments at the hearing to argue that the ECHR does not preclude national legislation providing, in essence, for a general and indiscriminate retention of traffic and location data, cannot call into question the interpretation of Article 15(1) of Directive 2002/58 resulting from the foregoing considerations. Those judgments concerned the bulk interception of data relating to international communications. Thus, as the Commission observed at the hearing, the European Court of Human Rights did not rule, in those judgments, on the compatibility with the ECHR of a general and indiscriminate retention of traffic and location data on national territory or even a large-scale interception of those data for the purposes of the prevention, detection and investigation of serious criminal offences. In any event, it should be borne in mind that Article 52(3) of the Charter is intended to ensure the necessary consistency between the rights contained in the Charter and the corresponding rights guaranteed in the ECHR, without adversely affecting the autonomy of EU law and that of the Court of Justice of the European Union, with the result that, for the purpose of interpreting the Charter, account must be taken of the corresponding rights of the ECHR only as the minimum threshold of protection (judgment of 17 December 2020,   
Centraal Israëlitisch Consistorie van België and Others  
, C-336/19, EU:C:2020:1031, paragraph 56).  
   
Access to data that have been retained in a general and indiscriminate way  
126    At the hearing, the Danish Government argued that the competent national authorities should be able to access, for the purpose of combating serious crime, traffic and location data that have been retained in a general and indiscriminate way, in accordance with the case-law arising from the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 to 139), in order to confront a serious threat to national security which is shown to be genuine and present or foreseeable.  
127    It should be observed, first of all, that authorising access, for the purpose of combating serious crime, to traffic and location data which have been retained in a general and indiscriminate way would make that access depend upon circumstances unrelated to that objective, according to whether or not, in the Member State concerned, there was a serious threat to national security as referred to in the preceding paragraph, whereas, in view of the sole objective of the fight against serious crime which must justify the retention of those data and access thereto, there is nothing to justify a difference in treatment, in particular as between the Member States (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 97).  
128    As the Court has already held, access to traffic and location data retained by providers of electronic communications services in accordance with a measure taken under Article 15(1) of Directive 2002/58, which must be given effect in full compliance with the conditions resulting from the case-law interpreting that directive, may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data. It is otherwise only if the importance of the objective pursued by access is greater than that of the objective which justified retention (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 98).  
129    The Danish Government’s argument refers to a situation in which the objective pursued by the access request proposed, namely the fight against serious crime, is of lesser importance in the hierarchy of objectives of public interest than that which justified the retention, namely the safeguarding of national security. To authorise, in that situation, access to retained data would be contrary to that hierarchy of public interest objectives recalled in the preceding paragraph and in paragraphs 68, 71, 72 and 73 above (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 99).  
130    In addition and moreover, in accordance with the case-law recalled in paragraph 74 above, traffic and location data cannot be the object of general and indiscriminate retention for the purpose of combating serious crime and, therefore, access to those data cannot be justified for that same purpose. Where those data have exceptionally been retained in a general and indiscriminate way for the purpose of safeguarding national security against a genuine and present or foreseeable threat, in the circumstances referred to in paragraph 71 above, the national authorities competent to undertake criminal investigations cannot access those data in the context of criminal proceedings, without depriving of any effectiveness the prohibition on such retention for the purpose of combating serious crime, recalled in paragraph 74 above (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 100).  
131    In the light of all of the foregoing considerations, the answer to the question referred for a preliminary ruling is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislative measures which provide, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data. However, that Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as not precluding national legislative measures that:  
–        allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;  
–        provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;  
–        provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;  
–        provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;  
–        allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,  
provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.  
   
Costs  
132    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union,  
must be interpreted as meaning that:  
it precludes national legislative measures which provide, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data;  
it does not preclude legislative measures that:  
–          
allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;  
–          
provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;  
–          
provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;  
–          
provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;  
–          
allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,  
provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

ID: ce6ccd5b-dbbe-4293-945e-1537646395e8

Judgment of 21 Dec 2016, C-203/15 (  
Tele2 Sverige  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Location data   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
E-privacy Directive   
 >   
Electronic communications   
 >   
Confidentiality of electronic communications   
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Location data   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
   
JUDGMENT OF THE COURT (Grand Chamber)  
21 December 2016 (\*)  
(Reference for a preliminary ruling — Electronic communications — Processing of personal data — Confidentiality of electronic communications — Protection — Directive 2002/58/EC — Articles 5, 6 and 9 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 11 and Article 52(1) — National legislation — Providers of electronic communications services — Obligation relating to the general and indiscriminate retention of traffic and location data — National authorities — Access to data — No prior review by a court or independent administrative authority — Compatibility with EU law)  
In Joined Cases C-203/15 and C-698/15,  
REQUESTS for a preliminary ruling under Article 267 TFEU, made by the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England & Wales) (Civil Division) (United Kingdom), by decisions, respectively, of 29 April 2015 and 9 December 2015, received at the Court on 4 May 2015 and 28 December 2015, in the proceedings  
Tele2 Sverige AB  
 (C-203/15)  
v  
Post- och telestyrelsen,  
and  
Secretary of State for the Home Department  
 (C-698/15)  
v  
Tom Watson,  
Peter Brice,  
Geoffrey Lewis,  
interveners:  
Open Rights Group,  
Privacy International,  
The Law Society of England and Wales,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Tizzano, Vice-President, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), J.L. da Cruz Vilaça, E. Juhász and M. Vilaras, Presidents of the Chamber, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen and C. Lycourgos, Judges,  
Advocate General: H. Saugmandsgaard Øe,  
Registrar: C. Strömholm, Administrator,  
having regard to the decision of the President of the Court of 1 February 2016 that Case C-698/15 should be determined pursuant to the expedited procedure provided for in Article 105(1) of the Rules of Procedure of the Court,  
having regard to the written procedure and further to the hearing on 12 April 2016,  
after considering the observations submitted on behalf of:  
–        Tele2 Sverige AB, by M. Johansson and N. Torgerzon, advokater, and by E. Lagerlöf and S. Backman,  
–        Mr Watson, by J. Welch and E. Norton, Solicitors, I. Steele, Advocate, B. Jaffey, Barrister, and D. Rose QC,  
–        Mr Brice and Mr Lewis, by A. Suterwalla and R. de Mello, Barristers, R. Drabble QC, and S. Luke, Solicitor,  
–        Open Rights Group and Privacy International, by D. Carey, Solicitor, and by R. Mehta and J. Simor, Barristers,  
–        The Law Society of England and Wales, by T. Hickman, Barrister, and by N. Turner,  
–        the Swedish Government, by A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren and L. Swedenborg, acting as Agents,  
–        the United Kingdom Government, by S. Brandon, L. Christie and V. Kaye, acting as Agents, and by D. Beard QC, G. Facenna QC, J. Eadie QC and S. Ford, Barrister,   
–        the Belgian Government, by J.-C. Halleux, S. Vanrie and C. Pochet, acting as Agents,  
–        the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,  
–        the Danish Government, by C. Thorning and M. Wolff, acting as Agents,  
–        the German Government, by T. Henze, M. Hellmann and J. Kemper, acting as Agents, and by M. Kottmann and U. Karpenstein, Rechtsanwalte,  
–        the Estonian Government, by K. Kraavi-Käerdi, acting as Agent,  
–        Ireland, by E. Creedon, L. Williams and A. Joyce, acting as Agents, and by D. Fennelly BL,  
–        the Spanish Government, by A. Rubio González, acting as Agent,  
–        the French Government, by G. de Bergues, D. Colas, F.-X. Bréchot and C. David, acting as Agents,  
–        the Cypriot Government, by K. Kleanthous, acting as Agent,  
–        the Hungarian Government, by M. Fehér and G. Koós, acting as Agents,  
–        the Netherlands Government, by M. Bulterman, M. Gijzen and. J. Langer, acting as Agents,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Finnish Government, by J. Heliskoski, acting as Agent,  
–        the European Commission, by H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira and J. Vondung, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 19 July 2016,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The requests have been made in two proceedings between (i) Tele2 Sverige AB and Post- och telestyrelsen (the Swedish Post and Telecom Authority; ‘PTS’), concerning an order sent by PTS to Tele2 Sverige requiring the latter to retain traffic and location data in relation to its subscribers and registered users (Case C-203/15), and (ii) Mr Tom Watson, Mr Peter Brice and Mr Geoffrey Lewis, on the one hand, and the Secretary of State for the Home Department (United Kingdom of Great Britain and Northern Ireland), on the other, concerning the conformity with EU law of Section 1 of the Data Retention and Investigatory Powers Act 2014 (‘DRIPA’) (Case C-698/15).  
   
Legal context  
   
EU law  
 Directive 2002/58  
3        Recitals 2, 6, 7, 11, 21, 22, 26 and 30 of Directive 2002/58 state:  
‘(2)      This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by [the Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.  
...  
(6)      The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.  
(7)      In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.  
...  
(11)      Like Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.  
...  
(21)      Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.  
(22)      The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. ...  
...  
(26)      The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data … may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber’s right not to give or to withdraw his/her consent to such processing. ...  
...  
(30)      Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. ...’  
4        Article 1 of Directive 2002/58, headed ‘Scope and aim’, provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.  
2.      The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.  
3.      This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.’  
5        Article 2 of Directive 2002/58, headed ‘Definitions’, provides:  
‘Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.  
The following definitions shall also apply:  
...  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  
(c)      “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
...’  
6        Article 3 of Directive 2002/58, headed ‘Services concerned’, provides:  
‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.’  
7        Article 4 of that directive, headed ‘Security of processing’, is worded as follows:   
‘1.      The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.  
1a.               Without prejudice to Directive [95/46], the measures referred to in paragraph 1 shall at least:  
–        ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,  
–        protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and  
–        ensure the implementation of a security policy with respect to the processing of personal data.  
...’  
8        Article 5 of Directive 2002/58, headed ‘Confidentiality of the communications’, provides:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
...  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
9        Article 6 of Directive 2002/58, headed ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
...  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.’  
10      Article 9(1) of that directive, that article being headed ‘Location data other than traffic data’, provides:  
‘Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …’  
11      Article 15 of that directive, headed ‘Application of certain provisions of Directive [95/46]’, states:  
‘1.      Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.  
...  
1b.      Providers shall establish internal procedures for responding to requests for access to users’ personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.  
2.      The provisions of Chapter III on judicial remedies, liability and sanctions of Directive [95/46] shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.  
...’  
 Directive 95/46  
12      Article 22 of Directive 95/46, which is in Chapter III of that directive, is worded as follows:   
‘Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.’  
 Directive 2006/24/EC  
13      Article 1(2) of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), that article being headed ‘Subject matter and scope’, provided:  
‘This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.’  
14      Article 3 of that directive, headed ‘Obligation to retain data’, provided:  
‘1.      By way of derogation from Articles 5, 6 and 9 of [Directive 2002/58], Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.  
2.       The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.’  
   
Swedish law  
15      It is apparent from the order for reference in Case C-203/15 that the Swedish legislature, in order to transpose Directive 2006/24 into national law, amended the lagen (2003:389) om elektronisk kommunikation [Law (2003:389) on electronic communications; ‘the LEK’] and the förordningen (2003:396) om elektronisk kommunikation [Regulation (2003:396) on electronic communications]. Both of those texts, in the versions applicable to the dispute in the main proceedings, contain rules on the retention of electronic communications data and on access to that data by the national authorities.  
16      Access to that data is, in addition, regulated by the lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Law (2012:278) on gathering of data relating to electronic communications as part of intelligence gathering by law enforcement authorities: ‘Law 2012:278’) and by the rättegångsbalken (Code of Judicial Procedure; ‘the RB’).  
 The obligation to retain electronic communications data   
17      According to the information provided by the referring court in Case C-203/15, the provisions of Paragraph 16a of Chapter 6 of the LEK, read together with Paragraph 1 of Chapter 2 of that law, impose an obligation on providers of electronic communications services to retain data the retention of which was required by Directive 2006/24. The data concerned is that relating to subscriptions and all electronic communications necessary to trace and identify the source and destination of a communication; to determine its date, time, and type; to identify the communications equipment used and to establish the location of mobile communication equipment used at the start and end of each communication. The data which there is an obligation to retain is data generated or processed in the context of telephony services, telephony services which use a mobile connection, electronic messaging systems, internet access services and internet access capacity (connection mode) provision services. The obligation extends to data relating to unsuccessful communications. The obligation does not however extend to the content of communications.  
18      Articles 38 to 43 of Regulation (2003:396) on electronic communications specify the categories of data that must be retained. As regards telephony services, there is the obligation to retain data relating to calls and numbers called and the identifiable dates and times of the start and end of the communication. As regards telephony services which use a mobile connection, additional obligations are imposed, covering, for example, the retention of location data at the start and end of the communication. As regards telephony services using an IP packet, data to be retained includes, in addition to data mentioned above, data relating to the IP addresses of the caller and the person called. As regards electronic messaging systems, data to be retained includes data relating to the numbers of senders and recipients, IP addresses or other messaging addresses. As regards internet access services, data to be retained includes, for example, data relating to the IP addresses of users and the traceable dates and times of logging into and out of the internet access service.  
 Data retention period  
19      In accordance with Paragraph 16d of Chapter 6 of the LEK, the data covered by Paragraph 16a of that Chapter must be retained by the providers of electronic communications services for six months from the date of the end of communication. The data must then be immediately erased, unless otherwise provided in the second subparagraph of Paragraph 16d of that Chapter.  
 Access to retained data  
20      Access to retained data by the national authorities is governed by the provisions of Law 2012:278, the LEK and the RB.  
–       Law 2012:278  
21      In the context of intelligence gathering, the national police, the Säkerhetspolisen (the Swedish Security Service), and the Tullverket (the Swedish Customs Authority) may, on the basis of Paragraph 1 of Law 2012:278, on the conditions prescribed by that law and without informing the provider of an electronic communications network or a provider of an electronic communications service authorised under the LEK, undertake the collection of data relating to messages transmitted by an electronic communications network, the electronic communications equipment located in a specified geographical area and the geographical areas(s) where electronic communications equipment is or was located.  
22      In accordance with Paragraphs 2 and 3 of Law 2012:278, data may, as a general rule, be collected if, depending on the circumstances, the measure is particularly necessary in order to avert, prevent or detect criminal activity involving one or more offences punishable by a term of imprisonment of at least two years, or one of the acts listed in Paragraph 3 of that law, referring to offences punishable by a term of imprisonment of less than two years. Any grounds supporting that measure must outweigh considerations relating to the harm or prejudice that may be caused to the person affected by that measure or to an interest opposing that measure. In accordance with Paragraph 5 of that law, the duration of the measure must not exceed one month.  
23      The decision to implement such a measure is to be taken by the director of the authority concerned or by a person to whom that responsibility is delegated. The decision is not subject to prior review by a judicial authority or an independent administrative authority.  
24      Under Paragraph 6 of Law 2012:278, the Säkerhets och integritetsskyddsnämnden (the Swedish Commission on Security and Integrity Protection) must be informed of any decision authorising the collection of data. In accordance with Paragraph 1 of Lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Law (2007:980) on the supervision of certain law enforcement activities), that authority is to oversee the application of the legislation by the law enforcement authorities.  
–       The LEK  
25      Under Paragraph 22, first subparagraph, point 2, of Chapter 6 of the LEK, all providers of electronic communications services must disclose data relating to a subscription at the request of the prosecution authority, the national police, the Security Service or any other public law enforcement authority, if that data is connected with a presumed criminal offence. On the information provided by the referring court in Case C-203/15, it is not necessary that the offence be a serious crime.  
–       The RB  
26      The RB governs the disclosure of retained data to the national authorities within the framework of preliminary investigations. In accordance with Paragraph 19 of Chapter 27 of the RB, ‘placing electronic communications under surveillance’ without the knowledge of third parties is, as a general rule, permitted within the framework of preliminary investigations that relate to, inter alia, offences punishable by a sentence of imprisonment of at least six months. The expression ‘placing electronic communications under surveillance’, under Paragraph 19 of Chapter 27 of the RB, means obtaining data without the knowledge of third parties that relates to a message transmitted by an electronic communications network, the electronic communications equipment located or having been located in a specific geographical area, and the geographical area(s) where specific electronic communications equipment is or has been located.  
27      According to what is stated by the referring court in Case C-203/15, information on the content of a message may not be obtained on the basis of Paragraph 19 of Chapter 27 of the RB. As a general rule, placing electronic communications under surveillance may be ordered, under Paragraph 20 of Chapter 27 of the RB, only where there are reasonable grounds for suspicion that an individual has committed an offence and that the measure is particularly necessary for the purposes of the investigation: the subject of that investigation must moreover be an offence punishable by a sentence of imprisonment of at least two years, or attempts, preparation or conspiracy to commit such an offence. In accordance with Paragraph 21 of Chapter 27 of the RB, the prosecutor must, other than in cases of urgency, request from the court with jurisdiction authority to place electronic communications under surveillance.  
 The security and protection of retained data  
28      Under Paragraph 3a of Chapter 6 of the LEK, providers of electronic communications services who are subject to an obligation to retain data must take appropriate technical and organisational measures to ensure the protection of data during processing. On the information provided by the referring court in Case C-203/15, Swedish law does not, however, make any provision as to where the data is to be retained.  
   
United Kingdom law  
 DRIPA  
29      Section 1 of DRIPA, headed ‘Powers for retention of relevant communications data subject to safeguards’, provides:  
‘(1)      The Secretary of State may by notice (a “retention notice”) require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 (purposes for which communications data may be obtained).  
(2)      A retention notice may:  
(a)      relate to a particular operator or any description of operators;  
(b)      require the retention of all data or any description of data;  
(c)      specify the period or periods for which data is to be retained;  
(d)      contain other requirements, or restrictions, in relation to the retention of data;  
(e)      make different provision for different purposes;  
(f)      relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.  
(3)      The Secretary of State may by regulations make further provision about the retention of relevant communications data.  
(4)      Such provision may, in particular, include provision about:  
(a)      requirements before giving a retention notice;  
(b)      the maximum period for which data is to be retained under a retention notice;  
(c)      the content, giving, coming into force, review, variation or revocation of a retention notice;  
(d)      the integrity, security or protection of, access to, or the disclosure or destruction of, data retained by virtue of this section;  
(e)      the enforcement of, or auditing compliance with, relevant requirements or restrictions;  
(f)      a code of practice in relation to relevant requirements or restrictions or relevant power;  
(g)      the reimbursement by the Secretary of State (with or without conditions) of expenses incurred by public telecommunications operators in complying with relevant requirements or restrictions;  
(h)      the [Data Retention (EC Directive) Regulations 2009] ceasing to have effect and the transition to the retention of data by virtue of this section.  
(5)      The maximum period provided for by virtue of subsection (4)(b) must not exceed 12 months beginning with such day as is specified in relation to the data concerned by regulations under subsection (3).  
...’  
30      Section 2 of DRIPA defines the expression ‘relevant communications data’ as meaning ‘communications data of the kind mentioned in the Schedule to the [Data Retention (EC Directive) Regulations 2009] so far as such data is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned’.  
 RIPA  
31      Section 21(4) of the Regulation of Investigatory Powers Act 2000 (‘RIPA’), that section being in Chapter II of that act and headed ‘Lawful acquisition and disclosure of communications data’, states:  
‘In this Chapter “communications data” means any of the following:  
(a)      any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;  
(b)      any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person:  
(i)      of any postal service or telecommunications service; or  
(ii)      in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;  
(c)      any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service’.  
32      On the information provided in the order for reference in Case C-698/15, that data includes ‘user location data’, but not data relating to the content of a communication.  
33      As regards access to retained data, Section 22 of RIPA provides:  
‘(1)      This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.  
(2)      It is necessary on grounds falling within this subsection to obtain communications data if it is necessary:   
(a)      in the interests of national security;  
(b)      for the purpose of preventing or detecting crime or of preventing disorder;  
(c)      in the interests of the economic well-being of the United Kingdom;  
(d)      in the interests of public safety;  
(e)      for the purpose of protecting public health;  
(f)      for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;  
(g)      or the purpose, in an emergency, of preventing death or injury or any damage to a person’s physical or mental health, or of mitigating any injury or damage to a person’s physical or mental health; or  
(h)      or any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.  
…  
(4)      Subject to subsection (5), where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator:  
(a)      if the operator is not already in possession of the data, to obtain the data; and  
(b)      in any case, to disclose all of the data in his possession or subsequently obtained by him.  
(5)      The designated person shall not grant an authorisation under subsection (3) or give a notice under subsection (4), unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data.’  
34      Under Section 65 of RIPA, complaints may be made to the Investigatory Powers Tribunal (United Kingdom) if there is reason to believe that data has been acquired inappropriately.  
 The Data Retention Regulations 2014  
35      The Data Retention Regulations 2014 (‘the 2014 Regulations’), adopted on the basis of DRIPA, are divided into three parts, Part 2 containing regulations 2 to 14 of that legislation. Regulation 4, headed ‘Retention notices’, provides:  
‘(1) A retention notice must specify:  
(a)      the public telecommunications operator (or description of operators) to whom it relates,  
(b)      the relevant communications data which is to be retained,  
(c)      the period or periods for which the data is to be retained,  
(d)      any other requirements, or any restrictions, in relation to the retention of the data.  
(2)      A retention notice must not require any data to be retained for more than 12 months beginning with:  
(a)      in the case of traffic data or service use data, the day of the communication concerned, and  
(b)      in the case of subscriber data, the day on which the person concerned leaves the telecommunications service concerned or (if earlier) the day on which the data is changed.  
...’  
36      Regulation 7 of the 2014 Regulations, headed ‘Data integrity and security’, provides:  
‘(1)      A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must:  
(a)      secure that the data is of the same integrity and subject to at least the same security and protection as the data on any system from which it is derived,  
(b)      secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and  
(c)      protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure.  
(2)      A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must destroy the data if the retention of the data ceases to be authorised by virtue of that section and is not otherwise authorised by law.  
(3)      The requirement in paragraph (2) to destroy the data is a requirement to delete the data in such a way as to make access to the data impossible.  
(4)      It is sufficient for the operator to make arrangements for the deletion of the data to take place at such monthly or shorter intervals as appear to the operator to be practicable.’  
37      Regulation 8 of the 2014 Regulations, headed Disclosure of retained data’, provides:  
‘(1)      A public telecommunications operator must put in place adequate security systems (including technical and organisational measures) governing access to communications data retained by virtue of section 1 of [DRIPA] in order to protect against any disclosure of a kind which does not fall within section 1(6)(a) of [DRIPA].  
(2)      A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must retain the data in such a way that it can be transmitted without undue delay in response to requests.’  
38      Regulation 9 of the 2014 Regulations, headed ‘Oversight by the Information Commissioner’, states:  
‘The Information Commissioner must audit compliance with requirements or restrictions imposed by this Part in relation to the integrity, security or destruction of data retained by virtue of section 1 of [DRIPA].’  
 The Code of Practice  
39      The Acquisition and Disclosure of Communications Data Code of Practice (‘the Code of Practice’) contains, in paragraphs 2.5 to 2.9 and 2.36 to 2.45, guidance on the necessity for and proportionality of obtaining communications data. As explained by the referring court in Case C-698/15, particular attention must, in accordance with paragraphs 3.72 to 3.77 of that code, be paid to necessity and proportionality where the communications data sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information.  
40      Under paragraph 3.78 to 3.84 of that code, a court order is required in the specific case of an application for communications data that is made in order to identify a journalist’s source. Under paragraphs 3.85 to 3.87 of that code, judicial approval is required when an application for access is made by local authorities. No authorisation, on the other hand, need be obtained from a court or any independent body with respect to access to communications data protected by legal professional privilege or relating to doctors of medicine, Members of Parliament or ministers of religion.  
41      Paragraph 7.1 of the Code of Practice provides that communications data acquired or obtained under the provisions of RIPA, and all copies, extracts and summaries of that data, must be handled and stored securely. In additions, the requirements of the Data Protection Act must be adhered to.  
42      In accordance with paragraph 7.18 of the Code of Practice, where a United Kingdom public authority is considering the possible disclosure to overseas authorities of communications data, it must, inter alia, consider whether that data will be adequately protected. However, it is stated in paragraph 7.22 of that code that a transfer of data to a third country may take place where that transfer is necessary for reasons of substantial public interest, even where the third country does not provide an adequate level of protection. On the information given by the referring court in Case C-698/15, the Secretary of State for the Home Department may issue a national security certificate that exempts certain data from the provisions of the legislation.  
43      In paragraph 8.1 of that code, it is stated that RIPA established the Interception of Communications Commissioner (United Kingdom), whose remit is, inter alia, to provide independent oversight of the exercise and performance of the powers and duties contained in Chapter II of Part I of RIPA. As is stated in paragraph 8.3 of the code, the Commissioner may, where he can ‘establish that an individual has been adversely affected by any wilful or reckless failure’, inform that individual of suspected unlawful use of powers.  
   
The disputes in the main proceedings and the questions referred for a preliminary ruling  
   
Case C-203/15  
44      On 9 April 2014, Tele2 Sverige, a provider of electronic communications services established in Sweden, informed the PTS that, following the ruling in the judgment of 8 April 2014,   
Digital Rights Ireland and Others  
 (C-293/12 and C-594/12; ‘the   
Digital Rights  
 judgment’, EU:C:2014:238) that Directive 2006/24 was invalid, it would cease, as from 14 April 2014, to retain electronic communications data, covered by the LEK, and that it would erase data retained prior to that date.  
45      On 15 April 2014, the Rikspolisstyrelsen (the Swedish National Police Authority, Sweden) sent to the PTS a complaint to the effect that Tele2 Sverige had ceased to send to it the data concerned.  
46      On 29 April 2014, the justitieminister (Swedish Minister for Justice) appointed a special reporter to examine the Swedish legislation at issue in the light of the   
Digital Rights  
 judgment. In a report dated 13 June 2014, entitled ‘Datalagring, EU-rätten och svensk rätt, Ds 2014:23’ (Data retention, EU law and Swedish law; ‘the 2014 report’), the special reporter concluded that the national legislation on the retention of data, as set out in Paragraphs 16a to 16f of the LEK, was not incompatible with either EU law or the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (‘the ECHR’). The special reporter emphasised that the   
Digital Rights  
 judgment could not be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle. From his perspective, neither should the   
Digital Rights  
 judgment be understood as meaning that the Court had established, in that judgment, a set of criteria all of which had to be satisfied if legislation was to be able to be regarded as proportionate. He considered that it was necessary to assess all the circumstances in order to determine the compatibility of the Swedish legislation with EU law, such as the extent of data retention in the light of the provisions on access to data, on the duration of retention, and on the protection and the security of data.  
47      On that basis, on 19 June 2014 the PTS informed Tele2 Sverige that it was in breach of its obligations under the national legislation in failing to retain the data covered by the LEK for six months, for the purpose of combating crime. By an order of 27 June 2014, the PTS ordered Tele2 Sverige to commence, by no later than 25 July 2014, the retention of that data.  
48      Tele2 Sverige considered that the 2014 report was based on a misinterpretation of the   
Digital Rights  
 judgment and that the obligation to retain data was in breach of the fundamental rights guaranteed by the Charter, and therefore brought an action before the Förvaltningsrätten i Stockholm (Administrative Court, Stockholm) challenging the order of 27 June 2014. Since that court dismissed the action, by judgment of 13 October 2014, Tele2 Sverige brought an appeal against that judgment before the referring court.  
49      In the opinion of the referring court, the compatibility of the Swedish legislation with EU law should be assessed with regard to Article 15(1) of Directive 2002/58. While that directive establishes the general rule that traffic and location data should be erased or made anonymous when no longer required for the transmission of a communication, Article 15(1) of that directive introduces a derogation from that general rule since it permits the Member States, where justified on one of the specified grounds, to restrict that obligation to erase or render anonymous, or even to make provision for the retention of data. Accordingly, EU law allows, in certain situations, the retention of electronic communications data.  
50      The referring court nonetheless seeks to ascertain whether a general and indiscriminate obligation to retain electronic communications data, such as that at issue in the main proceedings, is compatible, taking into consideration the   
Digital Rights  
 judgment, with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter. Given that the opinions of the parties differ on that point, it is necessary that the Court give an unequivocal ruling on whether, as maintained by Tele2 Sverige, the general and indiscriminate retention of electronic communications data is per se incompatible with Articles 7 and 8 and Article 52(1) of the Charter, or whether, as stated in the 2014 Report, the compatibility of such retention of data is to be assessed in the light of provisions relating to access to the data, the protection and security of the data and the duration of retention.  
51      In those circumstances the Kammarrätten i Stockholm (Administrative Court of Appeal of Stockholm, Sweden) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:  
‘(1)      Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime … compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?   
(2)      If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:  
(a)      access by the national authorities to the retained data is determined as [described in paragraphs 19 to 36 of the order for reference], and   
(b)      data protection and security requirements are regulated as [described in paragraphs 38 to 43 of the order for reference], and  
(c)      all relevant data is to be retained for six months, calculated as from the day when the communication is ended, and subsequently erased as [described in paragraph 37 of the order for reference]?’  
   
Case C-698/15  
52      Mr Watson, Mr Brice and Mr Lewis each lodged, before the High Court of Justice (England & Wales), Queen’s Bench Division (Divisional Court) (United Kingdom), applications for judicial review of the legality of Section 1 of DRIPA, claiming, inter alia, that that section is incompatible with Articles 7 and 8 of the Charter and Article 8 of the ECHR.  
53      By judgment of 17 July 2015, the High Court of Justice (England & Wales), Queen’s Bench Division (Divisional Court) held that the   
Digital Rights  
 judgment laid down ‘mandatory requirements of EU law’ applicable to the legislation of Member States on the retention of communications data and access to such data. According to the High Court of Justice, since the Court, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. It follows from the underlying logic of the   
Digital Rights  
 judgment that legislation that establishes a general body of rules for the retention of communications data is in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation is complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, Section 1 of DRIPA is not compatible with Articles 7 and 8 of the Charter in so far as it does not lay down clear and precise rules providing for access to and use of retained data and in so far as access to that data is not made dependent on prior review by a court or an independent administrative body.  
54      The Secretary of State for the Home Department brought an appeal against that judgment before the Court of Appeal (England & Wales) (Civil Division) (United Kingdom).  
55      That court states that Section 1(1) of DRIPA empowers the Secretary of State for the Home Department to adopt, without any prior authorisation from a court or an independent administrative body, a general regime requiring public telecommunications operators to retain all data relating to any postal service or any telecommunications service for a maximum period of 12 months if he/she considers that such a requirement is necessary and proportionate to achieve the purposes stated in the United Kingdom legislation. Even though that data does not include the content of a communication, it could be highly intrusive into the privacy of users of communications services.  
56      In the order for reference and in its judgment of 20 November 2015, delivered in the appeal procedure, wherein it decided to send to the Court this request for a preliminary ruling, the referring court considers that the national rules on the retention of data necessarily fall within the scope of Article 15(1) of Directive 2002/58 and must therefore conform to the requirements of the Charter. However, as stated in Article 1(3) of that directive, the EU legislature did not harmonise the rules relating to access to retained data.  
57      As regards the effect of the   
Digital Rights  
 judgment on the issues raised in the main proceedings, the referring court states that, in the case that gave rise to that judgment, the Court was considering the validity of Directive 2006/24 and not the validity of any national legislation. Having regard, inter alia, to the close relationship between the retention of data and access to that data, it was essential that that directive should incorporate a set of safeguards and that the   
Digital Rights  
 judgment should analyse, when examining the lawfulness of the data retention regime established by that directive, the rules relating to access to that data. The Court had not therefore intended to lay down, in that judgment, mandatory requirements applicable to national legislation on access to data that does not implement EU law. Further, the reasoning of the Court was closely linked to the objective pursued by Directive 2006/24. National legislation should, however, be assessed in the light of the objectives pursued by that legislation and its context.  
58      As regards the need to refer questions to the Court for a preliminary ruling, the referring court draws attention to the fact that, when the order for reference was issued, six courts in other Member States, five of those courts being courts of last resort, had declared national legislation to be invalid on the basis of the   
Digital Rights  
 judgment. The answer to the questions referred is therefore not obvious, although the answer is required to give a ruling on the cases brought before that court.  
59      In those circumstances, the Court of Appeal (England & Wales) (Civil Division) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:   
‘(1)      Does [the   
Digital Rights  
 judgment] (including, in particular, paragraphs 60 to 62 thereof) lay down mandatory requirements of EU law applicable to a Member State’s domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of [the Charter]?  
(2)      Does [the   
Digital Rights  
 judgment] expand the scope of Articles 7 and/or 8 of [the Charter] beyond that of Article 8 of the European Convention of Human Rights … as established in the jurisprudence of the European Court of Human Rights …?’  
   
The procedure before the Court  
60      By order of 1 February 2016,   
Davis and Others  
 (C-698/15, not published, EU:C:2016:70), the President of the Court decided to grant the request of the Court of Appeal (England & Wales) (Civil Division) that Case C-698/15 should be dealt with under the expedited procedure provided for in Article 105(1) of the Court’s Rules of Procedure.  
61      By decision of the President of the Court of 10 March 2016, Cases C-203/15 and C-698/15 were joined for the purposes of the oral part of the procedure and the judgment.  
   
Consideration of the questions referred for a preliminary ruling  
   
The first question in Case C-203/15  
62      By the first question in Case C-203/15, the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm) seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation such as that at issue in the main proceedings that provides, for the purpose of fighting crime, for general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communications.  
63      That question arises, in particular, from the fact that Directive 2006/24, which the national legislation at issue in the main proceedings was intended to transpose, was declared to be invalid by the   
Digital Rights  
 judgment, though the parties disagree on the scope of that judgment and its effect on that legislation, given that it governs the retention of traffic and location data and access to that data by the national authorities.  
64      It is necessary first to examine whether national legislation such as that at issue in the main proceeding falls within the scope of EU law.  
 The scope of Directive 2002/58  
65      The Member States that have submitted written observations to the Court have differed in their opinions as to whether and to what extent national legislation on the retention of traffic and location data and access to that data by the national authorities, for the purpose of combating crime, falls within the scope of Directive 2002/58. Whereas, in particular, the Belgian, Danish, German and Estonian Governments, Ireland and the Netherlands Government have expressed the opinion that the answer is that it does, the Czech Government has proposed that the answer is that it does not, since the sole objective of such legislation is to combat crime. The United Kingdom Government, for its part, argues that only legislation relating to the retention of data, but not legislation relating to the access to that data by the competent national law enforcement authorities, falls within the scope of that directive.  
66      As regards, finally, the Commission, while it maintained, in its written observations submitted to the Court in Case C-203/15, that the national legislation at issue in the main proceedings falls within the scope of Directive 2002/58, the Commission argues, in its written observations in Case C-698/15, that only national rules relating to the retention of data, and not those relating to the access of the national authorities to that data, fall within the scope of that directive. The latter rules should, however, according to the Commission, be taken into consideration in order to assess whether national legislation governing the retention of data by providers of electronic communications services constitutes a proportionate interference in the fundamental rights guaranteed in Articles 7 and 8 of the Charter.  
67      In that regard, it must be observed that a determination of the scope of Directive 2002/58 must take into consideration, inter alia, the general structure of that directive.  
68      Article 1(1) of Directive 2002/58 indicates that the directive provides, inter alia, for the harmonisation of the provisions of national law required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector.  
69      Article 1(3) of that directive excludes from its scope ‘activities of the State’ in specified fields, including the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters (see, by analogy, with respect to the first indent of Article 3(2) of Directive 95/46, judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 43, and of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 41).  
70      Article 3 of Directive 2002/58 states that the directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices (‘electronic communications services’). Consequently, that directive must be regarded as regulating the activities of the providers of such services.  
71      Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, ‘legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 [of that directive]’. The second sentence of Article 15(1) of that directive identifies, as an example of measures that may thus be adopted by Member States, measures ‘providing for the retention of data’.  
72      Admittedly, the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 51). Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive.  
73      However, having regard to the general structure of Directive 2002/58, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.  
74      Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services. Accordingly, Article 15(1), read together with Article 3 of that directive, must be interpreted as meaning that such legislative measures fall within the scope of that directive.  
75      The scope of that directive extends, in particular, to a legislative measure, such as that at issue in the main proceedings, that requires such providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data.  
76      The scope of that directive also extends to a legislative measure relating, as in the main proceedings, to the access of the national authorities to the data retained by the providers of electronic communications services.   
77      The protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including ‘any data related to such communications’, in order to protect the confidentiality of electronic communications.  
78      In those circumstances, a legislative measure whereby a Member State, on the basis of Article 15(1) of Directive 2002/58, requires providers of electronic communications services, for the purposes set out in that provision, to grant national authorities, on the conditions laid down in such a measure, access to the data retained by those providers, concerns the processing of personal data by those providers, and that processing falls within the scope of that directive.  
79      Further, since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services.  
80      That interpretation is confirmed by Article 15(1b) of Directive 2002/58, which provides that providers are to establish internal procedures for responding to requests for access to users’ personal data, based on provisions of national law adopted pursuant to Article 15(1) of that directive.  
81      It follows from the foregoing that national legislation, such as that at issue in the main proceedings in Cases C-203/15 and C-698/15, falls within the scope of Directive 2002/58.  
 The interpretation of Article 15(1) of Directive 2002/58, in the light of Articles 7, 8, 11 and Article 52(1) of the Charter  
82      It must be observed that, according to Article 1(2) of Directive 2002/58, the provisions of that directive ‘particularise and complement’ Directive 95/46. As stated in its recital 2, Directive 2002/58 seeks to ensure, in particular, full respect for the rights set out in Articles 7 and 8 of the Charter. In that regard, it is clear from the explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which led to Directive 2002/58, that the EU legislature sought ‘to ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used’.  
83      To that end, Directive 2002/58 contains specific provisions designed, as is apparent from, in particular, recitals 6 and 7 of that directive, to offer to the users of electronic communications services protection against risks to their personal data and privacy that arise from new technology and the increasing capacity for automated storage and processing of data.  
84      In particular, Article 5(1) of that directive provides that the Member States must ensure, by means of their national legislation, the confidentiality of communications effected by means of a public communications network and publicly available electronic communications services, and the confidentiality of the related traffic data.  
85      The principle of confidentiality of communications established by Directive 2002/58 implies, inter alia, as stated in the second sentence of Article 5(1) of that directive, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 47).  
86      Accordingly, as confirmed by recitals 22 and 26 of Directive 2002/58, under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and for the time necessary for the billing and marketing of services and the provision of value added services (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraphs 47 and 48). As regards, in particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers obtained.  
87      The scope of Article 5, Article 6 and Article 9(1) of Directive 2002/58, which seek to ensure the confidentiality of communications and related data, and to minimise the risks of misuse, must moreover be assessed in the light of recital 30 of that directive, which states: ‘Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum’.  
88      Admittedly, Article 15(1) of Directive 2002/58 enables the Member States to introduce exceptions to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to in Articles 6 and 9 of that directive (see, to that effect, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 50).  
89      Nonetheless, in so far as Article 15(1) of Directive 2002/58 enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data, that provision must, in accordance with the Court’s settled case-law, be interpreted strictly (see, by analogy, judgment of 22 November 2012,   
Probst  
, C-119/12, EU:C:2012:748, paragraph 23). That provision cannot, therefore, permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58, to become the rule, if the latter provision is not to be rendered largely meaningless.  
90      It must, in that regard, be observed that the first sentence of Article 15(1) of Directive 2002/58 provides that the objectives pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be ‘to safeguard national security — that is, State security — defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system’, or one of the other objectives specified in Article 13(1) of Directive 95/46, to which the first sentence of Article 15(1) of Directive 2002/58 refers (see, to that effect, judgment of 29 January 2008,  
 Promusicae  
, C-275/06, EU:C:2008:54, paragraph 53). That list of objectives is exhaustive, as is apparent from the second sentence of Article 15(1) of Directive 2002/58, which states that the legislative measures must be justified on ‘the grounds laid down’ in the first sentence of Article 15(1) of that directive. Accordingly, the Member States cannot adopt such measures for purposes other than those listed in that latter provision.  
91      Further, the third sentence of Article 15(1) of Directive 2002/58 provides that ‘[a]ll the measures referred to [in Article 15(1)] shall be in accordance with the general principles of [European Union] law, including those referred to in Article 6(1) and (2) [EU]’, which include the general principles and fundamental rights now guaranteed by the Charter. Article 15(1) of Directive 2002/58 must, therefore, be interpreted in the light of the fundamental rights guaranteed by the Charter (see, by analogy, in relation to Directive 95/46, judgments of 20 May 2003,   
Österreichischer Rundfunk and Others  
, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; of 13 May 2014,   
Google Spain and Google  
, C-131/12, EU:C:2014:317, paragraph 68, and of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 38).  
92      In that regard, it must be emphasised that the obligation imposed on providers of electronic communications services, by national legislation such as that at issue in the main proceedings, to retain traffic data in order, when necessary, to make that data available to the competent national authorities, raises questions relating to compatibility not only with Articles 7 and 8 of the Charter, which are expressly referred to in the questions referred for a preliminary ruling, but also with the freedom of expression guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraphs 25 and 70).  
93      Accordingly, the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 of the Charter, as derived from the Court’s case-law (see, to that effect, judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 39 and the case-law cited), must be taken into consideration in interpreting Article 15(1) of Directive 2002/58. The same is true of the right to freedom of expression in the light of the particular importance accorded to that freedom in any democratic society. That fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 12 June 2003,   
Schmidberger  
, C-112/00, EU:C:2003:333, paragraph 79, and of 6 September 2011,   
Patriciello  
, C-163/10, EU:C:2011:543, paragraph 31).  
94      In that regard, it must be recalled that, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 15 February 2016,   
N.  
, C-601/15 PPU, EU:C:2016:84, paragraph 50).  
95      With respect to that last issue, the first sentence of Article 15(1) of Directive 2002/58 provides that Member States may adopt a measure that derogates from the principle of confidentiality of communications and related traffic data where it is a ‘necessary, appropriate and proportionate measure within a democratic society’, in view of the objectives laid down in that provision. As regards recital 11 of that directive, it states that a measure of that kind must be ‘strictly’ proportionate to the intended purpose. In relation to, in particular, the retention of data, the requirement laid down in the second sentence of Article 15(1) of that directive is that data should be retained ‘for a limited period’ and be ‘justified’ by reference to one of the objectives stated in the first sentence of Article 15(1) of that directive.  
96      Due regard to the principle of proportionality also derives from the Court’s settled case-law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary (judgments of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 56; of 9 November 2010,   
Volker und Markus Schecke and Eifert  
, C-92/09 and C-93/09, EU:C:2010:662, paragraph 77; the   
Digital Rights   
judgment, paragraph 52, and of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 92).  
97      As regards whether national legislation, such as that at issue in Case C-203/15, satisfies those conditions, it must be observed that that legislation provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions. As stated in the order for reference, the categories of data covered by that legislation correspond, in essence, to the data whose retention was required by Directive 2006/24.  
98      The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users’ communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period (see, by analogy, with respect to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 26).  
99      That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights judgment  
, paragraph 27). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.  
100    The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 37).  
101    Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 39), the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights   
judgment, paragraph 28).   
102    Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 60).  
103    Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 51).  
104    In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.  
105    Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraphs 57 and 58).  
106    Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 59).  
107    National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.  
108    However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.   
109    In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 54 and the case-law cited).  
110    Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.  
111    As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.  
112    Having regard to all of the foregoing, the answer to the first question referred in Case C-203/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.  
   
The second question in Case C-203/15 and the first question in Case C-698/15  
113    It must, at the outset, be noted that the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm) referred the second question in Case C-203/15 only in the event that the answer to the first question in that case was negative. That second question, however, arises irrespective of whether retention of data is generalised or targeted, as set out in paragraphs 108 to 111 of this judgment. Accordingly, the Court must answer the second question in Case C-203/15 together with the first question in Case C-698/15, which is referred regardless of the extent of the obligation to retain data that is imposed on providers of electronic communications services.  
114    By the second question in Case C-203/15 and the first question in Case C-698/15, the referring courts seek, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data, and more particularly, the access of the competent national authorities to retained data, where that legislation does not restrict that access solely to the objective of fighting serious crime, where that access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.  
115    As regards objectives that are capable of justifying national legislation that derogates from the principle of confidentiality of electronic communications, it must be borne in mind that, since, as stated in paragraphs 90 and 102 of this judgment, the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, access to the retained data must correspond, genuinely and strictly, to one of those objectives. Further, since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data.  
116    As regards compatibility with the principle of proportionality, national legislation governing the conditions under which the providers of electronic communications services must grant the competent national authorities access to the retained data must ensure, in accordance with what was stated in paragraphs 95 and 96 of this judgment, that such access does not exceed the limits of what is strictly necessary.  
117    Further, since the legislative measures referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, ‘be subject to adequate safeguards’, a data retention measure must, as follows from the case-law cited in paragraph 109 of this judgment, lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.  
118    In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 61).  
119    Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime (see, by analogy, ECtHR, 4 December 2015,   
Zakharov v. Russia  
, CE:ECHR:2015:1204JUD004714306, § 260). However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.  
120    In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016,   
Szabó and Vissy v. Hungary  
, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80).  
121    Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009,   
Rijkeboer  
, C-553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraph 95).  
122    With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the   
Digital Rights  
 judgment, paragraphs 66 to 68).  
123    In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court’s settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, the   
Digital Rights  
 judgment, paragraph 68, and the judgment of 6 October 2015,   
Schrems  
, C-362/14, EU:C:2015:650, paragraphs 41 and 58).  
124    It is the task of the referring courts to determine whether and to what extent the national legislation at issue in the main proceedings satisfies the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as set out in paragraphs 115 to 123 of this judgment, with respect to both the access of the competent national authorities to the retained data and the protection and level of security of that data.  
125    Having regard to all of the foregoing, the answer to the second question in Case C-203/15 and to the first question in Case C-698/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.  
   
The second question in Case C-698/15  
126    By the second question in Case C-698/15, the Court of Appeal (England & Wales) (Civil Division) seeks in essence to ascertain whether, in the   
Digital Rights  
 judgment, the Court interpreted Articles 7 and/or 8 of the Charter in such a way as to expand the scope conferred on Article 8 ECHR by the European Court of Human Rights.  
127    As a preliminary point, it should be recalled that, whilst, as Article 6(3) TEU confirms, fundamental rights recognised by the ECHR constitute general principles of EU law, the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law (see, to that effect, judgment of 15 February 2016,   
N.  
, C-601/15 PPU, EU:C:2016:84, paragraph 45 and the case-law cited).  
128    Accordingly, the interpretation of Directive 2002/58, which is at issue in this case, must be undertaken solely in the light of the fundamental rights guaranteed by the Charter (see, to that effect, judgment of 15 February 2016,   
N.  
, C-601/15 PPU, EU:C:2016:84, paragraph 46 and the case-law cited).  
129    Further, it must be borne in mind that the explanation on Article 52 of the Charter indicates that paragraph 3 of that article is intended to ensure the necessary consistency between the Charter and the ECHR, ‘without thereby adversely affecting the autonomy of Union law and … that of the Court of Justice of the European Union’ (judgment of 15 February 2016,   
N.  
, C-601/15 PPU, EU:C:2016:84, paragraph 47). In particular, as expressly stated in the second sentence of Article 52(3) of the Charter, the first sentence of Article 52(3) does not preclude Union law from providing protection that is more extensive then the ECHR. It should be added, finally, that Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR.  
130    However, in accordance with the Court’s settled case-law, the justification for making a request for a preliminary ruling is not for advisory opinions to be delivered on general or hypothetical questions, but rather that it is necessary for the effective resolution of a dispute concerning EU law (see, to that effect, judgments of 24 April 2012,   
Kamberaj  
, C-571/10, EU:C:2012:233, paragraph 41; of 26 February 2013,   
Åkerberg Fransson  
, C-617/10, EU:C:2013:105, paragraph 42, and of 27 February 2014,   
Pohotovosť  
, C-470/12, EU:C:2014:101 paragraph 29).  
131    In this case, in view of the considerations set out, in particular, in paragraphs 128 and 129 of the present judgment, the question whether the protection conferred by Articles 7 and 8 of the Charter is wider than that guaranteed in Article 8 of the ECHR is not such as to affect the interpretation of Directive 2002/58, read in the light of the Charter, which is the matter in dispute in the proceedings in Case C-698/15.  
132    Accordingly, it does not appear that an answer to the second question in Case C-698/15 can provide any interpretation of points of EU law that is required for the resolution, in the light of that law, of that dispute.  
133    It follows that the second question in Case C-698/15 is inadmissible.  
   
Costs  
134    Since these proceedings are, for the parties to the main proceedings, a step in the actions pending before the national courts, the decision on costs is a matter for those courts. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.  
2.        
Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.  
3.        
The second question referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible.  
Lenaerts   
Tizzano  
Silva de Lapuerta  
von Danwitz   
Da Cruz Vilaça   
Juhász  
Vilaras   
Borg Barthet  
Malenovský  
Levits  
Bonichot  
Arabadjiev  
Rodin  
Biltgen   
Lycourgos  
Delivered in open court in Luxembourg on 21 December 2016.  
A. Calot Escobar  
   
      K. Lenaerts  
Registrar  
   
      President  
\*\* Languages of the case: English and Swedish.  
   
  
  
  
  
Disclaimer

ID: d10d80a4-ea98-4cbe-8e2f-5f917dfa878f

of 22 Jun 2022, C-534/20 (  
Leistritz  
)  
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Data protection officer   
   
JUDGMENT OF THE COURT (First Chamber)  
22 June 2022 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Second sentence of Article 38(3) – Data protection officer – Prohibition of the dismissal, by a controller or processor, of a data protection officer or of the imposition, by a controller or processor, of a penalty on him or her for performing his or her tasks – Legal basis – Article 16 TFEU – Requirement of functional independence – National legislation prohibiting the termination of a data protection officer’s employment contract without just cause)  
In Case C-534/20,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesarbeitsgericht (Federal Labour Court, Germany), made by decision of 30 July 2020, received at the Court on 21 October 2020, in the proceedings  
Leistritz AG  
v  
LH,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, I. Ziemele (Rapporteur) and P.G. Xuereb, Judges,  
Advocate General: J. Richard de la Tour,  
Registrar: D. Dittert, Head of Unit,  
having regard to the written procedure and further to the hearing on 18 November 2021,  
after considering the observations submitted on behalf of:  
–        Leistritz AG, by O. Seeling and C. Wencker, Rechtsanwälte,  
–        LH, by S. Lohneis, Rechtsanwalt,  
–        the German Government, by J. Möller and S.K. Costanzo, acting as Agents,  
–        the Romanian Government, by E. Gane, acting as Agent,  
–        the European Parliament, by O. Hrstková Šolcová, P. López-Carceller and B. Schäfer, acting as Agents,  
–        the Council of the European Union, by T. Haas and K. Pleśniak, acting as Agents,  
–        the European Commission, by K. Herrmann, H. Kranenborg and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 27 January 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation and validity of the second sentence of Article 38(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2; ‘the GDPR’).  
2        The request has been made in proceedings between Leistritz AG and LH, who performed the duties of a data protection officer within that company, concerning the termination of her employment contract on account of a departmental reorganisation of that company.  
   
Legal context  
   
European Union law  
3        Recitals 10 and 97 of the GDPR state:  
‘(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
…  
(97)      … [The] data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.’  
4        Article 37 of the GDPR, entitled ‘Designation of the data protection officer’, reads as follows:  
‘1.      The controller and the processor shall designate a data protection officer in any case where:  
(a)      the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;  
(b)      the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or  
(c)      the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.  
…  
6.      The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.  
…’  
5        Article 38 of the GDPR, entitled ‘Position of the data protection officer’, provides, in paragraphs 3 and 5:  
‘3.      The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his [or her] tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.  
…  
5.      The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.’  
6        Article 39 of the GDPR, entitled ‘Tasks of the data protection officer’, provides in paragraph 1(b):  
‘The data protection officer shall have at least the following tasks:  
…  
(b)      to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;  
…’  
   
German law  
7        Paragraph 6 of the Bundesdatenschutzgesetz (Federal Law on data protection) of 20 December 1990 (BGBl. 1990 I, p. 2954), in the version in force from 25 May 2018 until 25 November 2019 (BGBl. 2017 I, p. 2097) (‘the BDSG’), entitled ‘Position’, provides in subparagraph 4:  
‘The dismissal of the data protection officer shall be permitted only by applying Paragraph 626 of the Bürgerliches Gesetzbuch [(German Civil Code), in the version of 2 January 2002 (BGBl. 2002 I, p. 42, corrigenda BGBl. 2002 I, p. 2909, and BGBl. 2003 I, p. 738)] accordingly. The data protection officer’s employment shall not be terminated unless there are facts that give the public body just cause to terminate without notice. The data protection officer’s employment shall not be terminated for one year after the activity as the data protection officer has ended, unless the public body has just cause to terminate without notice.’  
8        Paragraph 38 of the BDSG, entitled ‘Data protection officers of private bodies’, provides:  
‘(1)      In addition to Article 37(1)(b) and (c) of the [GDPR], the controller and processor shall designate a data protection officer if they generally continuously employ at least ten persons dealing with the automated processing of personal data. …  
(2)      Paragraph 6(4), (5), second sentence, and (6) shall apply; however, Paragraph 6(4) shall apply only if the designation of a data protection officer is mandatory.’  
9        Paragraph 134 of the Civil Code, in the version published on 2 January 2002 (‘the Civil Code’), entitled ‘Statutory prohibition’, reads as follows:  
‘Any legal act contrary to a statutory prohibition shall be void except as otherwise provided by law.’  
10      Paragraph 626 of the Civil Code, entitled ‘Termination without notice with just cause’, provides:  
‘(1)      The employment relationship may be terminated by either party to the contract with just cause without giving notice where facts are present on the basis of which the terminating party cannot reasonably be expected to continue the employment relationship to the end of the notice period or to the agreed end of the employment relationship, taking all circumstances of the individual case into account and weighing the interests of both parties to the contract.  
(2)      Termination may take place only upon expiry of a period of two weeks. That period starts to run when the person entitled to terminate becomes aware of the facts serving as the basis for termination. …’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
11      Leistritz is a company governed by private law, which is required under German law to designate a data protection officer. LH performed the duties of ‘head of legal affairs’ within that company from 15 January 2018 and those of data protection officer from 1 February 2018.  
12      By letter of 13 July 2018, Leistritz terminated LH’s employment contract with notice, with effect from 15 August 2018, invoking a restructuring measure of that company, in the context of which the activity of internal legal adviser and the data protection service were to be outsourced.  
13      The courts adjudicating on the substance, before which LH challenged the validity of the termination of her contract, ruled that that termination was invalid, since, in accordance with the combined provisions of Paragraph 38(2) and the second sentence of Paragraph 6(4) of the BDSG, LH’s contract could be terminated extraordinarily only if there was just cause, owing to her status as data protection officer. The restructuring measure described by Leistritz did not, they found, constitute such a cause.  
14      The referring court, before which Leistritz has brought an appeal on a point of law (‘  
Revision  
’), observes that, under German law, the termination of LH’s contract is void pursuant to those provisions and Paragraph 134 of the Civil Code. Nonetheless, it points out that the applicability of Paragraph 38(2) and of the second sentence of Paragraph 6(4) of the BDSG depends on whether EU law, and in particular the second sentence of Article 38(3) of the GDPR, allows legislation of a Member State to make the termination of a data protection officer’s employment contract subject to stricter conditions than those provided for by EU law. If it does not, the referring court would have to uphold the appeal on a point of law.  
15      The referring court states that its doubts arise particularly from the existence of a divergence in the national legal literature. On the one hand, the majority view considers that the special protection against termination provided for by the combined provisions of Paragraph 38(2) and the second sentence of Paragraph 6(4) of the BDSG constitutes a substantive rule of employment law in respect of which the European Union does not have legislative competence, with the result that those provisions are not contrary to the second sentence of Article 38(3) of the GDPR. On the other hand, according to the proponents of the minority view, the links between that protection and the position of data protection officer conflict with EU law and give rise to economic pressure to retain a data protection officer on a long-term basis once he or she has been designated.  
16      In those circumstances, the Bundesarbeitsgericht (Federal Labour Court, Germany) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is the second sentence of Article 38(3) of [the GDPR] to be interpreted as precluding a provision in national law, such as Paragraph 38(1) and (2) in conjunction with the second sentence of Paragraph 6(4) of the [BDSG], which declares ordinary termination of the employment contract of the data protection officer by the data controller, who is his or her employer, to be impermissible, irrespective of whether his or her contract is terminated for performing his or her tasks?  
If the first question is answered in the affirmative:  
(2)      Does the second sentence of Article 38(3) of the GDPR also preclude such a provision in national law if the designation of the data protection officer is not mandatory in accordance with Article 37(1) of the GDPR, but is mandatory only in accordance with the law of the Member State?  
If the first question is answered in the affirmative:  
(3)      Is the second sentence of Article 38(3) of the GDPR based on a sufficient enabling clause, in particular in so far as this covers data protection officers that are party to an employment contract with the data controller?’  
   
Consideration of the questions referred  
   
The first question  
17      By its first question, the referring court asks, in essence, whether the second sentence of Article 38(3) of the GDPR must be interpreted as precluding national legislation which provides that a controller or a processor may terminate the employment contract of a data protection officer, who is a member of his or her staff, only with just cause, even if the contractual termination is not related to the performance of that officer’s tasks.  
18      As is clear from settled case-law, in interpreting a provision of EU law, it is necessary to consider not only its wording, by considering the latter’s usual meaning in everyday language, but also the context in which the provision occurs and the objectives pursued by the rules of which it is part (judgment of 22 February 2022  
, Stichting Rookpreventie Jeugd and Others  
, C-160/20, EU:C:2022:101, paragraph 29 and the case-law cited).  
19      In the first place, as regards the wording of the provision at issue, it should be noted that Article 38(3) of the GDPR provides, in its second sentence, that ‘he or she shall not be dismissed or penalised by the controller or the processor for performing his [or her] tasks’.  
20      At the outset, it should be noted that the GDPR does not define the terms ‘dismissed’, ‘penalised’ and ‘for performing his [or her] tasks’ featuring in the second sentence of Article 38(3).  
21      That being so, first, in accordance with the meaning which those words have in everyday language, the prohibition of the dismissal, by a controller or processor, of a data protection officer or of the imposition, by a controller or processor, of a penalty on him or her means, as the Advocate General essentially observed in points 24 and 26 of his Opinion, that that officer must be protected against any decision terminating his or her duties, by which he or she would be placed at a disadvantage or which would constitute a penalty.  
22      In that regard, a measure terminating a data protection officer’s employment contract taken by his or her employer and terminating the employment relationship existing between that officer and that employer and, therefore, also terminating the function of data protection officer in the undertaking concerned may constitute such a decision.  
23      Second, the second sentence of Article 38(3) of the GDPR clearly applies without distinction both to the data protection officer who is a member of the staff of the controller or processor and to the person who fulfils the tasks on the basis of a service contract concluded with the latter, in accordance with Article 37(6) of the GDPR.  
24      It follows that the second sentence of Article 38(3) of the GDPR is intended to apply to the relationship between a data protection officer and a controller or processor, irrespective of the nature of the employment relationship between that controller and the latter.  
25      Third, it should be noted that that provision imposes a limit which consists, as the Advocate General stated, in essence, in point 29 of his Opinion, in prohibiting the termination of a data protection officer’s employment contract on a ground relating to the performance of his or her tasks, which include, in particular, under Article 39(1)(b) of the GDPR, monitoring compliance with EU or Member State legal provisions and with the policies of the controller or processor in relation to the protection of personal data.  
26      In the second place, as regards the objective pursued by the second sentence of Article 38(3) of the GDPR, it must first be pointed out that recital 97 of that regulation states that data protection officers, whether or not they are employees of the controller, should be in a position to perform their duties and tasks in an independent manner. In that regard, such independence must necessarily enable them to carry out those tasks in accordance with the objective of the GDPR, which seeks, inter alia, as is apparent from recital 10 thereof, to ensure a high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 207 and the case-law cited).  
27      Second, the objective of ensuring the functional independence of the data protection officer, as it follows from the second sentence of Article 38(3) of the GDPR, is also apparent from the first and third sentences of that provision, which require that that officer is not to receive any instructions regarding the exercise of those tasks and is to report directly to the highest level of management of the controller or processor, and from Article 38(5), which provides that, with regard to that exercise, that officer is to be bound by secrecy or confidentiality.  
28      Thus, the second sentence of Article 38(3) of the GDPR, by protecting the data protection officer against any decision which terminates his or her duties, places him or her at a disadvantage or constitutes a penalty, where such a decision relates to the performance of his or her tasks, must be regarded as essentially seeking to preserve the functional independence of the data protection officer and, therefore, to ensure that the provisions of the GDPR are effective. By contrast, that provision is not intended to govern the overall employment relationship between a controller or a processor and staff members who are likely to be affected only incidentally, to the extent strictly necessary for the achievement of those objectives.  
29      That interpretation is supported, in the third place, by the context of that provision and, in particular, by the legal basis on which the EU legislature adopted the GDPR.  
30      As is apparent from the preamble to the GDPR, that regulation was adopted on the basis of Article 16 TFEU, paragraph 2 of which provides, in particular, that the European Parliament and the Council of the European Union are, by means of regulations, acting in accordance with the ordinary legislative procedure, to lay down the rules relating, first, to the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices or agencies and by the Member States when carrying out activities which fall within the scope of EU law and, second, to the free movement of such data.  
31      By contrast, apart from the specific protection of the data protection officer provided for in the second sentence of Article 38(3) of the GDPR, the fixing of rules on protection against the termination of the employment contract of a data protection officer employed by a controller or by a processor does not fall within the scope of the protection of natural persons with regard to the processing of personal data or within the scope of the free movement of such data, but within the field of social policy.  
32      In that regard, it should be borne in mind, first, that, under Article 4(2)(b) TFEU, the European Union and the Member States have, in the field of social policy, for the aspects defined in that Treaty, a shared competence for the purposes of Article 2(2) thereof. Second, and as is specified in Article 153(1)(d) TFEU, the European Union is to support and complement the activities of the Member States in the field of the protection of workers in cases where their employment contract is terminated (see, by analogy judgment of 19 November 2019,   
TSN and AKT  
, C-609/17 and C-610/17, EU:C:2019:981, paragraph 47).  
33      That being so, as is clear from Article 153(2)(b) TFEU, it is by means of directives that the Parliament and the Council may lay down minimum requirements in that regard, since such minimum requirements cannot, according to the Court’s case-law, in the light of Article 153(4) TFEU, prevent any Member State from maintaining or introducing more stringent protective measures that are compatible with the Treaties (see, to that effect judgment of 19 November 2019,   
TSN and AKT  
, C-609/17 and C-610/17, EU:C:2019:981, paragraph 48).  
34      It follows, as the Advocate General stated, in essence, in point 44 of his Opinion, that each Member State is free, in the exercise of its retained competence, to lay down more protective specific provisions on the termination of a data protection officer’s employment contract, in so far as those provisions are compatible with EU law and, in particular, with the provisions of the GDPR, particularly the second sentence of Article 38(3) thereof.  
35      In particular, as the Advocate General observed in points 50 and 51 of his Opinion, such increased protection cannot undermine the achievement of the objectives of the GDPR. That would be the case if it prevented any termination of the employment contract, by a controller or by a processor, of a data protection officer who no longer possesses the professional qualities required to perform his or her tasks or who does not fulfil those tasks in accordance with the provisions of the GDPR.  
36      In the light of the foregoing considerations, the answer to the first question is that the second sentence of Article 38(3) of the GDPR must be interpreted as not precluding national legislation which provides that a controller or a processor may terminate the employment contract of a data protection officer, who is a member of his or her staff, only with just cause, even if the contractual termination is not related to the performance of that officer’s tasks, in so far as such legislation does not undermine the achievement of the objectives of the GDPR.  
   
The second and third questions  
37      In the light of the answer given to the first question, there is no need to answer the second and third questions.  
   
Costs  
38      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
The second sentence of Article 38(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as not precluding national legislation which provides that a controller or a processor may terminate the employment contract of a data protection officer, who is a member of his or her staff, only with just cause, even if the contractual termination is not related to the performance of that officer’s tasks, in so far as such legislation does not undermine the achievement of the objectives of that regulation.

ID: d3a83386-70d9-49b2-bfd2-257aa52b1e68

of 22 Jun 2023, C-579/21 (  
Pankki S  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
   
JUDGMENT OF THE COURT (First Chamber)  
22 June 2023 (\*)  
(Reference for a preliminary ruling – Processing of personal data – Regulation (EU) 2016/679 – Articles 4 and 15 – Scope of the right of access to information referred to in Article 15 – Information contained in log data – Article 4 – Definition of ‘personal data’ – Definition of ‘recipients’ – Temporal application)  
In Case C-579/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Itä-Suomen hallinto-oikeus (Administrative Court of Eastern Finland, Finland), made by decision of 21 September 2021, received at the Court on 22 September 2021, in the proceedings brought by  
J.M.  
intervening parties:  
Apulaistietosuojavaltuutettu,  
Pankki S,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, P.G. Xuereb, T. von Danwitz, A. Kumin and I. Ziemele (Rapporteur), Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 12 October 2022,  
after considering the observations submitted on behalf of:  
–        J.M., by himself,  
–        the Apulaistietosuojavaltuutettu, par A. Talus, tietosuojavaltuutettu,  
–        Pankki S, by T. Kalliokoski and J. Lång, asianajajat, and by E.-L. Hokkonen, oikeustieteen maisteri,  
–        the Finnish Government, by A. Laine and H. Leppo, acting as Agents,  
–        the Czech Government, by A. Edelmannová, M. Smolek and J. Vláčil, acting as Agents,  
–        the Austrian Government, by A. Posch, acting as Agent,  
–        the European Commission, by A. Bouchagiar, H. Kranenborg and I. Söderlund, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 15 December 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 15(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (‘the GDPR’).  
2        The request has been made in proceedings brought by J.M. seeking annulment of the decision of the Apulaistietosuojavaltuutettu (Assistant Data Protection Supervisor, Finland) rejecting his request that Pankki S, a banking institution established in Finland, be ordered to communicate to him certain information in relation to consultation operations carried out on his personal data.  
   
Legal context  
3        Recitals 4, 10, 11, 26, 39, 58, 60, 63 and 74 of the GDPR state:  
‘(4)      The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; …  
…  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. …  
(11)      Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, …  
…  
(26)      … To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. …  
…  
(39)      Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. …  
…  
(58)      The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.  
…  
(60)      The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. …  
…  
(63)      A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. … Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. … That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. …  
…  
(74)      The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.’  
4        Article 1 of the GDPR, headed ‘Subject matter and objectives’, provides in paragraph 2 thereof:  
‘This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.’  
5        Article 4 of that regulation provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person …; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …  
…  
(9)      “recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. …  
…  
(21)      “supervisory authority” means an independent public authority which is established by a Member State pursuant to Article 51;  
…’   
6        Article 5 of that regulation, entitled ‘Principles relating to processing of personal data’, is worded as follows:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
…  
(f)      processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
7        Article 12 of the GDPR, entitled ‘Transparent information, communication and modalities for the exercise of the rights of the data subject’, states:  
‘1.      The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, … The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. …  
…  
5.      … Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:  
…  
(b)      refuse to act on the request.  
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.  
…’  
8        Article 15 of that regulation, entitled ‘Right of access by the data subject’, provides:  
‘1.      The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:  
(a)      the purposes of the processing;  
(b)      the categories of personal data concerned;  
(c)      the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;  
(d)      where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;  
(e)      the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;  
(f)      the right to lodge a complaint with a supervisory authority;  
(g)      where the personal data are not collected from the data subject, any available information as to their source;  
(h)      the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.  
…  
3.      The controller shall provide a copy of the personal data undergoing processing. …  
4.      The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.’  
9        Articles 16 and 17 of that regulation lay down, respectively, the data subject’s right to have inaccurate personal data rectified (right of rectification), as well as the right, in certain circumstances, to erasure of those data (right to erasure or ‘right to be forgotten’).  
10      Article 18 of that regulation, entitled ‘Right to restriction of processing’, provides in paragraph 1 thereof:  
‘The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:  
(a)      the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;  
(b)      the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;  
(c)      the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;  
(d)      the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.’  
11      Article 21 of the GDPR, entitled ‘Right to object’, provides in paragraph 1 thereof:  
‘The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.’  
12      Under Article 24(1) of that regulation:  
‘Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. …’  
13      Article 29 of that regulation, entitled ‘Processing under the authority of the controller or processor’, is worded as follows:  
‘The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.’  
14      Article 30 of the GDPR, entitled ‘Records of processing activities’, provides:  
‘1.      Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility. …  
…  
4.      The controller … and, where applicable, the controller’s … representative, shall make the record available to the supervisory authority on request.  
…’  
15      Article 58 of that regulation, entitled ‘Powers’, provides, in paragraph 1 thereof:  
‘Each supervisory authority shall have all of the following investigative powers:  
(a)      to order the controller and the processor, and, where applicable, the controller’s or the processor’s representative to provide any information it requires for the performance of its tasks;  
…’  
16      Article 77 of that regulation, entitled ‘Right to lodge a complaint with a supervisory authority’, states as follows:  
‘1.      Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.  
2.      The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.’  
17      Article 79 of the GDPR, entitled ‘Right to an effective judicial remedy against a controller or processor’, states in paragraph 1 thereof:  
‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’  
18      Article 82 of that regulation, entitled ‘Right to compensation and liability’, provides in paragraph 1 thereof:  
‘Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.’  
19      In accordance with Article 99(2) thereof, the GDPR has been applicable from 25 May 2018.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
20      In 2014, J.M., who was then an employee and customer of Pankki S, learned that his own customer data had been accessed by members of the bank’s staff on several occasions during the period from 1 November to 31 December 2013.  
21      Since he had doubts as to the lawfulness of those consultations, J.M., who had in the meantime been dismissed from his post with Pankki S, on 29 May 2018 asked Pankki S to inform him of the identity of the persons who had consulted his customer data, the exact dates of the consultations and the purposes for which those data were processed.  
22      In its reply of 30 August 2018, Pankki S, in its capacity as controller within the meaning of Article 4(7) of the GDPR, refused to disclose the identity of the employees who had carried out the consultation operations on the ground that that information constituted the personal data of those employees.  
23      However, in that reply, Pankki S provided further details of the consultation operations carried out, on its instructions, by its internal audit department. It thus explained that a customer of the bank in respect of whom J.M. was the customer advisor was a creditor of a person also bearing J.M.’s surname, so that the bank had wished to clarify whether the applicant in the main proceedings and the debtor in question were one and the same person and whether there might have been a possible impermissible conflict of interest. Pankki S added that the clarification of that issue required the processing of J.M.’s data, and every member of the bank’s staff who had processed his data had given a statement to the internal audit department on the reasons for the processing of the data. In addition, the bank stated that those consultations had made it possible to rule out any suspicion of conflict of interest in relation to J.M..  
24      J.M. applied to the Tietosuojavaltuutetun toimisto (Data Protection Supervisor’s Office, Finland), the supervisory authority within the meaning of Article 4(21) of the GDPR, for an order that Pankki S provide him with the information requested.  
25      By decision of 4 August 2020, the Assistant Data Protection Supervisor rejected J.M.’s application. He explained that such an application sought to enable J.M. to gain access to the log data of the employees who had processed his data, whereas, under the Assistant Data Protection Supervisor’s decision-making practice, such log data constituted personal data relating not to the person concerned but to the employees who processed the data of that person.  
26      J.M. brought an action against that decision before the referring court.  
27      That court notes that Article 15 of the GDPR provides for the right of the data subject to obtain from the controller access to the data processed concerning him or her and information relating, inter alia, to the purposes of the processing and recipients of the data. It asks whether the communication of the log data generated during processing operations, which contain such information, in particular the identity of the controller’s employees, is covered by Article 15 of the GDPR, since those log data might prove necessary to the data subject for the purposes of assessing the lawfulness of the processing of his or her data.  
28      In those circumstances, the Itä-Suomen hallinto-oikeus (Administrative Court of Eastern Finland) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is the data subject’s right of access under Article 15(1) of the [GDPR], considered in conjunction with the [concept of] “personal data” within the meaning of Article 4(1) thereof, to be interpreted as meaning that information collected by the controller, which indicates who processed the data subject’s personal data and when and for what purpose they were processed, does not constitute information in respect of which the data subject has a right of access, in particular because it consists of data concerning the controller’s employees?  
(2)      If Question 1 is answered in the affirmative and the data subject does not have a right of access to the information referred to in that question on the basis of Article 15(1) of the [GDPR], because it does not constitute “personal data” of the data subject within the meaning of Article 4(1) of [that regulation], it remains necessary in the present case to consider the information in respect of which the data subject does have a right of access in accordance with Article 15(1)[(a) to (h)]:  
(a)      How is the purpose of processing within the meaning of Article 15(1)(a) [of the GDPR] to be interpreted in relation to the scope of the data subject’s right of access, that is to say, can the purpose of the processing give rise to a right of access to the user log data collected by the controller, such as information concerning personal data of the processors and the time and the purpose of the processing of the personal data?  
(b)      In that context, can the persons who processed J.M.’s customer data be regarded, under certain criteria, as recipients of the personal data within the meaning of Article 15(1)(c) of the [GDPR], in respect of whom the data subject would be entitled to obtain information?  
(3)      Is the fact that the bank at issue performs a regulated activity or that J.M. was both an employee and a customer of the bank at the same time relevant to the present case?  
(4)      Is the fact that J.M.’s data were processed before the entry into force of the [GDPR] relevant to the examination of the questions set out above?’  
   
Consideration of the questions referred  
   
The fourth question  
29      By its fourth question, which it is appropriate to examine first, the referring court asks, in essence, whether Article 15 of the GDPR, read in the light of Article 99(2) of that regulation, is applicable to a request for access to the information referred to in the first of those provisions where the processing operations covered by that request were carried out before the date on which that regulation became applicable, but the request was made after that date.  
30      In order to answer that question, it should be noted that, under Article 99(2) of the GDPR, that regulation has been applicable since 25 May 2018.  
31      In the present case, it is apparent from the order for reference that the personal data processing operations at issue in the main proceedings were carried out between 1 November 2013 and 31 December 2013, that is to say, before the date on which the GDPR became applicable. However, it is also apparent from that decision that J.M. submitted his request for information to Pankki S after that date, namely on 29 May 2018.  
32      In that regard, it must be borne in mind that procedural rules are generally taken to apply from the date on which they enter into force, as opposed to substantive rules, which are usually interpreted as applying to situations that have arisen and become definitive before their entry into force only in so far as it follows clearly from their terms, their objectives or their general scheme that such an effect must be given to them (judgment of 15 June 2021,   
Facebook Ireland and Others  
, C-645/19, EU:C:2021:483, paragraph 100 and the case-law cited).  
33      In the present case, it is apparent from the order for reference that J.M.’s request to be provided with the information at issue in the main proceedings is connected with Article 15(1) of the GDPR, which provides for the right of the data subject to obtain access to personal data concerning him or her which are being processed, and to the information referred to in that provision.  
34      It must be stated that that provision does not concern the conditions under which the processing of the personal data of the data subject is lawful. Article 15(1) of the GDPR merely specifies the scope of that data subject’s right of access to the data and to the information to which it covers.  
35      It follows, as the Advocate General observed in point 33 of his Opinion, that Article 15(1) of the GDPR confers on data subjects a procedural right consisting of obtaining information about the processing of their personal data. As a procedural rule, that provision applies to requests for access made from the entry into application of that regulation, such as J.M.’s request.  
36      In those circumstances, the answer to the fourth question is that Article 15 of the GDPR, read in the light of Article 99(2) of that regulation, must be interpreted as meaning that it is applicable to a request for access to the information referred to in that provision where the processing operations which that request concerns were carried out before the date on which that regulation became applicable, but the request was submitted after that date.  
   
The first and second questions  
37      By its first and second questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of the GDPR must be interpreted as meaning that information relating to consultation operations carried out on a data subject’s personal data and concerning the dates and purposes of those operations, and the identity of the natural persons who carried out those operations, constitutes information which that data subject is entitled to obtain from the controller under that provision.  
38      As a preliminary point, it should be borne in mind that, in accordance with settled case-law, the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 12 January 2023,   
Österreichische Post (Information regarding the recipients of personal data)  
, C-154/21, EU:C:2023:3, point 29).  
39      As regards, first of all, the wording of Article 15(1) of the GDPR, that provision states that the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and information about the purposes of the processing and the recipients or categories of recipient to whom those personal data have been or will be disclosed.  
40      In that regard, it must be pointed out that the concepts in Article 15(1) of the GDPR are defined in Article 4 of that regulation.  
41      Thus, in the first place, Article 4(1) of the GDPR states that personal data is ‘any information relating to an identified or identifiable natural person’ and specifies that ‘an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.  
42      The use of the expression ‘any information’ in the definition of the concept of ‘personal data’ in that provision reflects the aim of the EU legislature to assign a wide scope to that concept, which potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it ‘relates’ to the data subject (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 23).  
43      In that regard, it has been held that information relates to an identified or identifiable natural person where, by reason of its content, purpose or effect, it is linked to an identifiable person (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 24).  
44      As regards the ‘identifiable’ nature of a person, recital 26 of the GDPR states that account should be taken of ‘all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly’.  
45      Therefore, the broad definition of the concept of ‘personal data’ covers not only data collected and stored by the controller, but also includes all information resulting from the processing of personal data relating to an identified or identifiable person (see, to that effect, judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 26).  
46      In the second place, as regards the concept of ‘processing’, as defined in Article 4(2) of the GDPR, it should be noted that, by using the expression ‘any operation’, the EU legislature intended to give that concept a broad scope by using a non-exhaustive list of operations applied to personal data or sets of personal data, which cover, among others, collection, recording, storage or also consultation (see, to that effect, judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 27).  
47      In the third place, Article 4(9) of the GDPR states that ‘recipient’ means ‘a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not’.  
48      In that regard, the Court has held that the data subject has the right to obtain from the controller information about the specific recipients to whom the personal data concerning him or her have been or will be disclosed (judgment of 12 January 2023,   
Österreichische Post (Information regarding the recipients of personal data)  
, C-154/21, EU:C:2023:3, paragraph 46).  
49      Therefore, it follows from the textual analysis of Article 15(1) of the GDPR and the concepts contained therein that the right of access granted to the data subject by that provision is characterised by the broad scope of the information that the controller must provide to the data subject.  
50      As regards, next, the context of Article 15(1) of the GDPR, in the first place, recital 63 of that regulation provides that every data subject should have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed and the recipients of the personal data.  
51      In the second place, recital 60 of the GDPR states that the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes, it being stressed that the controller should provide any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed. Furthermore, in accordance with the principle of transparency, alluded to by the referring court, to which recital 58 of the GDPR refers and which is expressly enshrined in Article 12(1) of that regulation, any information sent to the data subject must be concise, easily accessible and easy to understand, and formulated in clear and plain language.  
52      In that regard, Article 12(1) of the GDPR states that the information must be provided by the controller in writing or by other means, including, where appropriate, by electronic means, unless the data subject requests that it be provided orally. The purpose of that provision, an expression of the principle of transparency, is to ensure that the data subject is able fully to understand the information sent to him or her (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 38 and the case-law cited).  
53      It follows from the foregoing contextual analysis that Article 15(1) of the GDPR is one of the provisions intended to ensure the transparency of the manner in which personal data are processed in relation to the data subject.  
54      Lastly, that interpretation of the scope of the right of access provided for in Article 15(1) of the GDPR is supported by the objectives pursued by that regulation.  
55      First, as stated in recitals 10 and 11 thereof, the purpose of that regulation is to ensure a consistent and high level of protection of natural persons within the European Union and to strengthen and set out in detail the rights of data subjects.  
56      In addition, as is apparent from recital 63 of the GDPR, the right of a data subject to have access to his or her own personal data and to the other information referred to in Article 15(1) of that regulation is intended, first of all, to enable that person to become aware of the processing and to verify its lawfulness. It follows, according to that same recital and as stated in paragraph 50 above, that every data subject should have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data and the logic involved in their processing.  
57      In that regard, it must be recalled, secondly, that the Court has already held that the right of access provided for in Article 15 of the GDPR must enable the data subject to ensure that the personal data relating to him or her are correct and that they are processed in a lawful manner (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF,   
 C-487/21, EU:C:2023:369, paragraph 34).  
58      In particular, that right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her right to rectification, right to erasure (‘right to be forgotten’) or right to restriction of processing, conferred, respectively, by Articles 16 to 18 of the GDPR, as well as the data subject’s right to object to his or her personal data being processed, laid down in Article 21 of the GDPR, and right of action where he or she suffers damage, laid down in Articles 79 and 82 of the GDPR (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 35 and the case-law cited).  
59      Accordingly, Article 15(1) of the GDPR is one of the provisions intended to ensure transparency vis-à-vis the data subject of the manner in which personal data are processed (judgment of 12 January 2023,   
Österreichische Post (Information regarding the recipients of personal data)  
, C-154/21, EU:C:2023:3, paragraph 42), without which that data subject would not be in a position to assess the lawfulness of the processing of his or her data or to exercise the rights provided for, inter alia, in Articles 16 to 18, 21, 79 and 82 of that regulation.  
60      In the present case, it is apparent from the order for reference that J.M. requested Pankki S to provide him with information relating to the consultation operations carried out on his personal data between 1 November 2013 and 31 December 2013, including the dates of those consultations, their purposes and the identity of the persons who carried them out. The referring court states that the transmission of the log data generated during those operations would make it possible to respond to J.M’s request.  
61      Here, it is not disputed that the consultation operations carried out on the personal data of the applicant in the main proceedings constitute ‘processing’ within the meaning of Article 4(2) of the GDPR, with the result that they confer on him, pursuant to Article 15(1) of that regulation, not only a right of access to those personal data, but also a right to be provided with the information linked to those operations, as referred to in the latter provision.  
62      In respect of information such as that requested by J.M., the communication, first of all, of the dates of the consultation operations is such as to enable the data subject to obtain confirmation that his personal data have actually been processed at a given time. In addition, since the conditions of lawfulness laid down in Articles 5 and 6 of the GDPR must be satisfied at the point of the processing itself, the date of that processing is a factor which makes it possible to verify its lawfulness. Next, it should be noted that information relating to the purposes of the processing is expressly referred to in Article 15(1)(a) of that regulation. Lastly, Article 15(1)(c) of that regulation provides that the controller is to inform the data subject of the recipients to whom his or her data have been disclosed.  
63      As regards, specifically, the communication of all that information by means of the provision of the log data relating to the processing operations at issue in the main proceedings, it should be noted that the first sentence of Article 15(3) of the GDPR states that the controller ‘shall provide a copy of the personal data undergoing processing’.  
64      In that regard, the Court has already held that the concept of ‘copy’ thus used refers to the faithful reproduction or transcription of an original, with the result that a purely general description of the data undergoing processing or a reference to categories of personal data does not correspond to that definition. Furthermore, it is apparent from the wording of the first sentence of Article 15(3) of that regulation that the disclosure obligation relates to the personal data undergoing the processing in question (see, to that effect, judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 21).  
65      The copy that the controller is required to provide must contain all the personal data undergoing processing, must have all the characteristics necessary for the data subject effectively to exercise his or her rights under that regulation and must, consequently, reproduce those data fully and faithfully (see, to that effect, judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraphs 32 and 39).  
66      In order to ensure that the information thus provided is easy to understand, as required by Article 12(1) of the GDPR, read in conjunction with recital 58 of that regulation, the reproduction of extracts from documents or even entire documents or extracts from databases which contain, inter alia, the personal data undergoing processing may prove to be essential where the contextualisation of the data processed is necessary in order to ensure the data are intelligible. In particular, where personal data are generated from other data or where such data result from empty fields, that is to say, where there is an absence of information which provides information about the data subject, the context in which the data are processed is an essential element in enabling the data subject to have transparent access and an intelligible presentation of those data (judgment of 4 May 2023,  
 Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraphs 41 and 42).  
67      In the present case, as the Advocate General observed in points 88 to 90 of his Opinion, the log data, which contain the information requested by J.M., correspond to records of activities, within the meaning of Article 30 of the GDPR. It must be held that they fall within the scope of the measures, referred to in recital 74 of that regulation, implemented by the controller to demonstrate the compliance of the processing activities with that regulation. Article 30(4) of that regulation specifies in particular that they must be made available to the supervisory authority on its request.  
68      In so far as those records of activities do not contain information relating to an identified or identifiable natural person within the meaning of the case-law referred to in paragraphs 42 and 43 above, they merely enable the controller to fulfil his or her obligations towards the supervisory authority which requests the provision of those records.  
69      As regards, more specifically, the controller’s log data, the disclosure of a copy of the information contained in those files may be necessary in order to satisfy the obligation to provide the data subject with access to all the information referred to in Article 15(1) of the GDPR and to ensure fair and transparent processing, thus enabling him or her fully to assert his or her rights under that regulation.  
70      First, such log data reveal the existence of data processing, information to which the data subject must have access under Article 15(1) of the GDPR. In addition, they provide information on the frequency and intensity of the consultation operations, thus enabling the data subject to ensure that the processing carried out is actually motivated by the purposes put forward by the controller.  
71      Secondly, those files contain information relating to the identity of the persons who carried out the consultation operations.  
72      In the present case, it is apparent from the order for reference that the persons who carried out the consultation operations at issue in the main proceedings are employees of Pankki S, who acted under its authority and in accordance with its instructions.  
73      Although it follows from Article 15(1)(c) of the GDPR that the data subject has the right to obtain from the controller information relating to the recipients or categories of recipients to whom the personal data have been or will be disclosed, the employees of the controller cannot be regarded as being ‘recipients’, within the meaning of Article 15(1)(c) of the GDPR, as recalled in paragraphs 47 and 48 above, when they process personal data under the authority of that controller and in accordance with its instructions, as the Advocate General observed in point 63 of his Opinion.  
74      In that regard, it must be pointed out that, in accordance with Article 29 of the GDPR, any person acting under the authority of the controller who has access to personal data may process those data only on instructions from that controller.  
75      That being the case, the information contained in the log data relating to the persons who have consulted the data subject’s personal data could constitute information falling within the scope of Article 4(1) of the GDPR, as recalled in paragraph 41 above, capable of enabling him or her to verify the lawfulness of the processing of his or her data and, in particular, to satisfy him or herself that the processing operations were actually carried out under the authority of the controller and in accordance with its instructions.  
76      Nevertheless, first, it is apparent from the order for reference that the information in log data such as those at issue in the main proceedings makes it possible to identify the employees who carried out the processing operations and contains personal data of those employees, within the meaning of Article 4(1) of the GDPR.  
77      In that regard, it should be recalled that, as regards the right of access provided for in Article 15 of the GDPR, recital 63 of that regulation states that ‘that right should not adversely affect the rights or freedoms of others’.  
78      Under recital 4 of the GDPR, the right to the protection of personal data is not an absolute right, since it must be considered in relation to its function in society and be balanced against other fundamental rights (see, to that effect, judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 172).  
79      Even if the disclosure of the information relating to the identity of the controller’s employees to the data subject may be necessary for that data subject in order to ensure the lawfulness of the processing of his or her personal data, it is nevertheless liable to infringe the rights and freedoms of those employees.  
80      In those circumstances, in the event of a conflict between, on the one hand, the exercise of a right of access which ensures the effectiveness of the rights conferred on the data subject by the GDPR and, on the other hand, the rights or freedoms of others, a balance will have to be struck between the rights and freedoms in question. Wherever possible, means of communicating personal data that do not infringe the rights or freedoms of others should be chosen, bearing in mind that, as follows from recital 63 of the GDPR, ‘the result of those considerations should not be a refusal to provide all information to the data subject’ (see, to that effect, judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 44).  
81      However, secondly, it is apparent from the order for reference that J.M. does not seek disclosure of the information relating to the identity of Pankki S’s employees who carried out the consultation operations on his personal data on the ground that they did not actually act under the authority and in accordance with the instructions of the controller, but appears to doubt the veracity of the information relating to the purpose of those consultations communicated to him by Pankki S.  
82      In such circumstances, if the data subject were to consider the information provided by the controller to be insufficient to enable him or her to dispel his or her doubts as to the lawfulness of the processing of his or her personal data, he or she has the right to lodge a complaint with the supervisory authority on the basis of Article 77(1) of the GDPR, that authority having the power, under Article 58(1)(a) of that regulation, to request the controller to provide it with any information it needs in order to examine the data subject’s complaint.  
83      It follows from the foregoing considerations that Article 15(1) of the GDPR must be interpreted as meaning that information relating to consultation operations carried out on a data subject’s personal data and concerning the dates and purposes of those operations constitutes information which that person has the right to obtain from the controller under that provision. On the other hand, that provision does not lay down such a right in respect of information relating to the identity of the employees of that controller who carried out those operations under its authority and in accordance with its instructions, unless that information is essential in order to enable the data subject effectively to exercise the rights conferred on him or her by that regulation and provided that the rights and freedoms of those employees are taken into account.  
   
The third question  
84      By its third question, the referring court asks, in essence, whether the fact, first, that the controller is engaged in the business of banking and acts within the framework of a regulated activity and, second, that the data subject whose personal data has been processed in his or her capacity as a customer of the controller was also an employee of that controller is relevant for the purposes of defining the scope of the right of access conferred on him or her by Article 15(1) of the GDPR.  
85      At the outset, it should be noted that, as regards the scope of the right of access provided for in Article 15(1) of the GDPR, no provision of that regulation draws a distinction according to the nature of the activities of the controller or the status of the person whose personal data are being processed.  
86      As regards, first, the regulated nature of Pankki S’s activity, it is true that Article 23 of the GDPR allows Member States to restrict by way of a legislative measure the scope of the obligations and rights provided for, inter alia, in Article 15 of that regulation.  
87      However, it is not apparent from the order for reference that Pankki S’s activity is subject to such legislation.  
88      As regards, secondly, the fact that J.M. was both a customer and an employee of Pankki S, it should be noted that, having regard not only to the objectives of the GDPR but also to the scope of the data subject’s right of access, as recalled in paragraphs 49 and 55 to 59 above, the context in which that data subject requests access to the information referred to in Article 15(1) of the GDPR cannot have any influence on the scope of that right.  
89      Consequently, Article 15(1) of the GDPR must be interpreted as meaning that the fact that the controller is engaged in the business of banking and acts within the framework of a regulated activity and that the data subject whose personal data has been processed in his or her capacity as a customer of the controller was also an employee of that controller, in principle, has no effect on the scope of the right of access conferred on that data subject by that provision.  
   
Costs  
90      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
1.        
Article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), read in the light of Article 99(2) of that regulation,  
must be interpreted as meaning that it is applicable to a request for access to the information referred to in that provision where the processing operations which that request concerns were carried out before the date on which that regulation became applicable, but the request was submitted after that date.  
2.        
Article 15(1) of Regulation 2016/679  
must be interpreted as meaning that information relating to consultation operations carried out on a data subject’s personal data and concerning the dates and purposes of those operations constitutes information which that person has the right to obtain from the controller under that provision. On the other hand, that provision does not lay down such a right in respect of information relating to the identity of the employees of that controller who carried out those operations under its authority and in accordance with its instructions, unless that information is essential in order to enable the person concerned effectively to exercise the rights conferred on him or her by that regulation and provided that the rights and freedoms of those employees are taken into account.  
3.        
Article 15(1) of Regulation 2016/679  
must be interpreted as meaning that the fact that the controller is engaged in the business of banking and acts within the framework of a regulated activity and that the data subject whose personal data has been processed in his or her capacity as a customer of the controller was also an employee of that controller has, in principle, no effect on the scope of the right of access conferred on that data subject by that provision.

ID: d52d9562-f16a-48f4-8092-40ff6328003b

of 20 Sep 2022, C-339/20 (  
VD  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Data retention and access of national authorities   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
   
JUDGMENT OF THE COURT (Grand Chamber)  
20 September 2022 (\*)  
(References for a preliminary ruling – Single Market for financial services – Market abuse – Insider dealing – Directive 2003/6/EC – Article 12(2)(a) and (d) – Regulation (EU) No 596/2014 – Article 23(2)(g) and (h) – Supervisory and investigatory powers of the Autorité des marchés financiers (AMF) – General interest objective seeking to protect the integrity of financial markets in the European Union and public confidence in financial instruments – Option open to the AMF to require the traffic data records held by an operator providing electronic communications services – Processing of personal data in the electronic communications sector – Directive 2002/58/EC – Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Confidentiality of communications – Restrictions – Legislation providing for the general and indiscriminate retention of traffic data by operators providing electronic communications services – Option for a national court to restrict the temporal effects of a declaration of invalidity in respect of provisions of national law that are incompatible with EU law – Precluded)  
In Joined Cases C-339/20 and C-397/20,  
REQUESTS for a preliminary ruling under Article 267 TFEU from the Cour de cassation (Court of Cassation, France), made by decisions of 1 April 2020, received at the Court on 24 July 2020 and 20 August 2020 respectively, in the criminal proceedings against  
VD  
 (C-339/20),  
SR  
 (C-397/20),   
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis and I. Ziemele, Presidents of Chambers, T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (Rapporteur), N. Piçarra, L.S. Rossi and A. Kumin, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: R. Șereș, Administrator,  
having regard to the written procedure and further to the hearing on 14 September 2021,  
after considering the observations submitted on behalf of:  
–        VD, by D. Foussard and F. Peltier, avocats,  
–        SR, by M. Chavannes and P. Spinosi, avocats,  
–        the French Government, by A. Daniel, E. de Moustier, D. Dubois, J. Illouz and T. Stéhelin, acting as Agents,  
–        the Danish Government, by N. Holst-Christensen, N. Lykkegaard and M. Søndahl Wolff, acting as Agents,  
–        the Estonian Government, by A. Kalbus and M. Kriisa, acting as Agents,  
–        Ireland, by M. Browne, A. Joyce and J. Quaney, acting as Agents, and by D. Fennelly, Barrister-at-Law,  
–        the Spanish Government, by L. Aguilera Ruiz, acting as Agent,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Portuguese Government, by P. Barros da Costa, L. Inez Fernandes, L. Medeiros and I. Oliveira, acting as Agents,  
–        the European Commission, by S.L. Kalėda, H. Kranenborg, T. Scharf and F. Wilman, acting as Agents,  
–        the European Data Protection Supervisor, by A. Buchta, M. Guglielmetti, C.-A. Mamier and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 18 November 2021,  
gives the following  
Judgment  
1        These requests for a preliminary ruling concern, in essence, the interpretation of Article 12(2)(a) and (d) of Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) (OJ 2003 L 96, p. 16) and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (OJ 2014 L 173, p. 1), read in conjunction with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), and read in the light of Articles 7, 8 and 11 and of Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The requests have been made in the context of criminal proceedings brought against VD and SR in respect of insider dealing, concealment of insider dealing, aiding and abetting, corruption and money laundering.  
   
Legal context  
   
European Union law  
   
Directive 2002/58  
3        Recitals 2, 6, 7 and 11 of Directive 2002/58 state:  
‘(2)      This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the [Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.  
…  
(6)      The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.  
(7)      In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.  
…  
(11)      Like Directive [95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.’  
4        Article 1 of Directive 2002/58, headed ‘Scope and aim’, provides:  
‘1.      This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.  
2.      The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.  
3.      This Directive shall not apply to activities which fall outside the scope of the [FEU Treaty], such as those covered by Titles V and VI [of the EU Treaty], and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.’  
5        Article 2 of that directive, headed ‘Definitions’, provides in point (b) of the second paragraph:  
‘The following definitions shall … apply:  
…  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof’.  
6        Article 5 of the directive, headed ‘Confidentiality of the communications’, provides:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
2.      Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
7        Article 6 of Directive 2002/58, headed ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
…’  
8        Article 9 of that directive, headed ‘Location data other than traffic data’, provides, in paragraph 1 thereof:  
‘1.      Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …’  
9        Article 15 of Directive 2002/58, headed ‘Application of certain provisions of Directive [95/46]’, provides, in paragraph 1 thereof:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].’  
   
Directive 2003/6  
10      Recitals 1, 2, 12, 37, 41 and 44 of Directive 2003/6 are worded as follows:  
‘(1)      A genuine Single Market for financial services is crucial for economic growth and job creation in the Community.   
(2)      An integrated and efficient financial market requires market integrity. The smooth functioning of securities markets and public confidence in markets are prerequisites for economic growth and wealth. Market abuse harms the integrity of financial markets and public confidence in securities and derivatives.  
…  
(12)      Market abuse consists of insider dealing and market manipulation. The objective of legislation against insider dealing is the same as that of legislation against market manipulation: to ensure the integrity of Community financial markets and to enhance investor confidence in those markets. …   
…  
(37)      A common minimum set of effective tools and powers for the competent authority of each Member State will guarantee supervisory effectiveness. Market undertakings and all economic actors should also contribute at their level to market integrity. …  
…  
(41)      Since the objective of the proposed action, namely to prevent market abuse in the form of insider dealing and market manipulation, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the measures, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 [TEU]. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.  
(44)      This Directive respects the fundamental rights and observes the principles recognised in particular by [the Charter] and in particular by Article 11 thereof and Article 10 of the European Convention [for the Protection of] Human Rights [and Fundamental Freedoms]. …’  
11      Article 11 of that directive provides:  
‘Without prejudice to the competences of the judicial authorities, each Member State shall designate a single administrative authority competent to ensure that the provisions adopted pursuant to this Directive are applied.  
…’  
12      Article 12 of that directive provides:  
‘1.      The competent authority shall be given all supervisory and investigatory powers that are necessary for the exercise of its functions. …  
2.      Without prejudice to Article 6(7), the powers referred to in paragraph 1 of this Article shall be exercised in conformity with national law and shall include at least the right to:  
(a)      have access to any document in any form whatsoever, and to receive a copy of it;  
…  
(d)      require existing telephone and existing data traffic records;  
…’  
   
Regulation No 596/2014  
13      Regulation No 596/2014 repealed and replaced Directive 2003/6 with effect from 3 July 2016.  
14      Recitals 1, 2, 7, 24, 44, 62, 65, 66, 77 and 86 of that regulation are worded as follows:  
‘(1)      A genuine internal market for financial services is crucial for economic growth and job creation in the Union.  
(2)      An integrated, efficient and transparent financial market requires market integrity. The smooth functioning of securities markets and public confidence in markets are prerequisites for economic growth and wealth. Market abuse harms the integrity of financial markets and public confidence in securities and derivatives.  
…  
(7)      Market abuse is a concept that encompasses unlawful behaviour in the financial markets and, for the purposes of this Regulation, it should be understood to consist of insider dealing, unlawful disclosure of inside information and market manipulation. Such behaviour prevents full and proper market transparency, which is a prerequisite for trading for all economic actors in integrated financial markets.  
…  
(24)      Where a legal or natural person in possession of inside information acquires or disposes of, or attempts to acquire or dispose of, for his own account or for the account of a third party, directly or indirectly, financial instruments to which that information relates, it should be implied that that person has used that information. That presumption is without prejudice to the rights of the defence. The question whether a person has infringed the prohibition on insider dealing or has attempted to commit insider dealing should be analysed in the light of the purpose of this Regulation, which is to protect the integrity of the financial market and to enhance investor confidence, which is based, in turn, on the assurance that investors will be placed on an equal footing and protected from the misuse of inside information.  
…  
(44)      Many financial instruments are priced by reference to benchmarks. The actual or attempted manipulation of benchmarks, including interbank offer rates, can have a serious impact on market confidence and may result in significant losses to investors or distort the real economy. …  
…  
(62)      A set of effective tools and powers and resources for the competent authority of each Member State guarantees supervisory effectiveness. Accordingly, this Regulation, in particular, provides for a minimum set of supervisory and investigative powers competent authorities of Member States should be entrusted with under national law. Those powers should be exercised, where the national law so requires, by application to the competent judicial authorities. …  
…  
(65)      Existing recordings of telephone conversations and data traffic records from investment firms, credit institutions and financial institutions executing and documenting the execution of transactions, as well as existing telephone and data traffic records from telecommunications operators, constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing and market manipulation. Telephone and data traffic records may establish the identity of a person responsible for the dissemination of false or misleading information or that persons have been in contact at a certain time, and that a relationship exists between two or more people. Therefore, competent authorities should be able to require existing recordings of telephone conversations, electronic communications and data traffic records held by an investment firm, a credit institution or a financial institution in accordance with Directive 2014/65/EU [of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ 2014 L 173, p. 349)]. Access to data and telephone records is necessary to provide evidence and investigate leads on possible insider dealing or market manipulation, and therefore for detecting and imposing sanctions for market abuse. In order to introduce a level playing field in the Union in relation to the access to telephone and existing data traffic records held by a telecommunications operator or the existing recordings of telephone conversations and data traffic held by an investment firm, a credit institution or a financial institution, competent authorities should, in accordance with national law, be able to require existing telephone and existing data traffic records held by a telecommunications operator, in so far as permitted under national law and existing recordings of telephone conversations as well as data traffic held by an investment firm, in cases where a reasonable suspicion exists that such records related to the subject matter of the inspection or investigation may be relevant to prove insider dealing or market manipulation infringing this Regulation. Access to telephone and data traffic records held by a telecommunications operator does not encompass access to the content of voice communications by telephone.  
(66)      While this Regulation specifies a minimum set of powers competent authorities should have, those powers are to be exercised within a complete system of national law which guarantees the respect for fundamental rights, including the right to privacy. For the exercise of those powers, which may amount to serious interferences with the right to respect for private and family life, home and communications, Member States should have in place adequate and effective safeguards against any abuse, for instance, where appropriate a requirement to obtain prior authorisation from the judicial authorities of a Member State concerned. Member States should allow the possibility for competent authorities to exercise such intrusive powers to the extent necessary for the proper investigation of serious cases where there are no equivalent means for effectively achieving the same result.  
…  
(77)      This Regulation respects the fundamental rights and observes the principles recognised in the [Charter]. Accordingly, this Regulation should be interpreted and applied in accordance with those rights and principles. …  
…  
(86)      Since the objective of this Regulation, namely to prevent market abuse in the form of insider dealing, the unlawful disclosure of inside information and market manipulation, cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 [TEU]. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.’  
15      Under Article 1 of that regulation:  
‘This Regulation establishes a common regulatory framework on insider dealing, the unlawful disclosure of inside information and market manipulation (market abuse) as well as measures to prevent market abuse to ensure the integrity of financial markets in the Union and to enhance investor protection and confidence in those markets.’  
16      Under the heading ‘Definitions’, Article 3 of that regulation provides, in subparagraph (1)(27):  
‘For the purposes of this Regulation, the following definitions apply:   
…  
(27)      “data traffic records” means records of traffic data as defined in point (b) of the second paragraph of Article 2 of Directive [2002/58];’  
17      Under Article 14 of Regulation No 596/2014, headed ‘Prohibition of insider dealing and of unlawful disclosure of inside information’:  
‘A person shall not:  
(a)      engage or attempt to engage in insider dealing;  
(b)      recommend that another person engage in insider dealing or induce another person to engage in insider dealing; or  
(c)      unlawfully disclose inside information.’  
18      Article 22 of that regulation provides:  
‘Without prejudice to the competences of the judicial authorities, each Member State shall designate a single administrative competent authority for the purpose of this Regulation. …’  
19      Article 23 of that regulation, headed ‘Powers of competent authorities’, provides in paragraphs 2 and 3 thereof:  
‘2.      In order to fulfil their duties under this Regulation, competent authorities shall have, in accordance with national law, at least the following supervisory and investigatory powers:  
(a)      to access any document and data in any form, and to receive or take a copy thereof;  
…  
(g)      to require existing recordings of telephone conversations, electronic communications or data traffic records held by investment firms, credit institutions or financial institutions;  
(h)      to require, in so far as permitted by national law, existing data traffic records held by a telecommunications operator, where there is a reasonable suspicion of an infringement and where such records may be relevant to the investigation of an infringement of point (a) or (b) of Article 14 or Article 15;  
…  
3.      Member States shall ensure that appropriate measures are in place so that competent authorities have all the supervisory and investigatory powers that are necessary to fulfil their duties.  
…’  
   
French law  
   
The CPCE  
20      Article L. 34-1 of the Code des postes et des communications électroniques (Post and Electronic Communications Code), in the version applicable to the disputes in the main proceedings (‘the CPCE’), provided:  
‘I. – This Article shall apply to the processing of personal data in the course of the provision to the public of electronic communications services; it shall apply in particular to networks that support data collection and identification devices.  
II. – Electronic communications operators, in particular persons whose business is to provide access to online public communication services, shall erase or render anonymous any data relating to traffic, subject to the provisions contained in points III, IV, V and VI.  
Persons who provide electronic communications services to the public shall, with due regard for the provisions contained in the preceding paragraph, establish internal procedures for responding to requests from the competent authorities.  
Persons who, as a principal or ancillary business activity, provide to the public a connection allowing online communication via access to the network shall, including where this is offered free of charge, be subject to compliance with the provisions applicable to electronic communications operators under this Article.  
III. – For the purposes of investigating, detecting and prosecuting criminal offences or a failure to fulfil an obligation laid down in Article L. 336-3 of the code de la propriété intellectuelle (Intellectual Property Code) or for the purposes of preventing breaches of automated data processing systems as provided for and punishable under Articles 323-1 to 323-3-1 of the Code pénal (Criminal Code), and for the sole purpose of making information available, as necessary, to the judicial authority or high authority mentioned in Article L. 331-12 of the Intellectual Property Code or to the national authority for the security of information systems mentioned in Article L. 2321-1 of the code de la défense (Defence Code), operations designed to erase or render anonymous certain categories of technical data may be deferred for a maximum period of one year. A decree to be adopted following consultation of the Conseil d’État (Council of State, France) and the Data Protection Authority shall, within the limits laid down in point VI, determine the categories of data involved and the period for which they are to be retained, depending on the business of the operators, the nature of the communications and the methods of offsetting any identifiable and specific additional costs associated with the services provided for these purposes by operators at the request of the State.  
…  
VI. – Data retained and processed under the conditions set out in points III, IV and V shall relate exclusively to the identification of persons using the services provided by operators, the technical characteristics of the communications provided by the latter and the location of terminal equipment.  
Under no circumstance may such data relate to the content of the correspondence or the information consulted, in any form whatsoever, as part of those communications.  
The retention and processing of such data shall be effected with due regard for the provisions of loi no 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés (Law No 78-17 of 6 January 1978 on information technology, files and freedoms).  
Operators shall take any measures necessary to prevent such data from being used for purposes other than those provided for in this Article.’  
21      Article L. 34-1 of the Post and Electronic Communications Code, in the version resulting from loi no 2021-998, du 30 juillet 2021, relative à la prévention d’actes de terrorisme et au renseignement (Law No 2021-998 of 30 July 2021 on the prevention of terrorist acts and information) (JORF of 31 July 2021, text No 1), provides in points II bis to III bis:  
‘II bis – Electronic communications operators shall retain:  
1.      For the purposes of criminal proceedings, the prevention of threats to public security and the safeguarding of national security, information on the user’s civil identity for a period of five years from the end of the term of his or her contract;  
2.      For the same purposes as those set out in point II bis(1), the other information provided by the user when entering into a contract or setting up an account and the payment information, for a period of one year from the end of the term of his or her contract or of the closure of his or her account;  
3.      For the purposes of combating crime and serious crime, the prevention of serious threats to public security and the safeguarding of national security, technical data that make it possible to identify the source of the connection or data relating to the terminal equipment used, for a period of one year from the connection or use of terminal equipment.  
III. – For reasons relating to the safeguarding of national security, where there is a serious, present or foreseeable threat to national security, the Prime Minister may, by decree, order electronic communication operators to retain for a period of one year certain categories of traffic data, in addition to the data referred to in point II bis(3), and location data specified by a decree to be adopted after consultation of the Conseil d’État (Council of State).  
The Prime Minister’s order, which may be applicable for up to one year, may be renewed if the conditions laid down for its enactment continue to be met. Its expiry shall have no effect on the data retention period referred to in the first paragraph of this point III.  
III bis – Data retained by operators under this Article may be subject to an expedited retention order issued by the authorities having access, under the law, to electronic communications data for the purposes of preventing and punishing crime, serious crime and other serious breaches of rules the observance of which they are responsible for ensuring, in order that those authorities may access those data.’  
22      Article R. 10-13 of the CPCE is worded as follows:  
‘I. – Pursuant to point III of Article L. 34-1, electronic communications operators shall retain the following data for the purposes of investigating, detecting and prosecuting criminal offences:  
(a)      information identifying the user;  
(b)      data relating to the communications terminal equipment used;  
(c)      the technical characteristics and date, time and duration of each communication;  
(d)      data relating to the additional services requested or used and the providers of those services;  
(e)      data identifying the addressee or addressees of the communication.  
II. – In the case of telephony activities, the operator shall retain the data referred to in point II and, additionally, data enabling the origin and location of the communication to be identified.  
III. – The data referred to in this Article shall be retained for one year from the date of registration.  
…’  
   
The LCEN  
23      Article 6 of Loi no 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique (Law No 2004-575 of 21 June 2004 to promote trust in the digital economy) (JORF of 22 June 2004, p. 11168), in the version applicable to the disputes in the main proceedings (‘the LCEN’) provided:  
‘I – 1.      Persons whose business is to provide access to online public communication services shall inform their subscribers of the existence of technical tools enabling access to some services to be restricted or for a selection of those services to be made and shall offer them at least one of those tools.  
…  
2.      Natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services, may not incur any civil liability for the activities or information stored at the request of a recipient of those services if they had no actual knowledge of either the unlawful nature of the activities or information in question or of the facts and circumstances pointing to their unlawful nature, or if, as soon as they became aware of that unlawful nature, they acted expeditiously to remove the data at issue or block access to them.  
…  
II. – The persons referred to in point I(1) and (2) shall keep and retain the data in such a way as to make it possible to identify anyone who has assisted in the creation of all or part of the content of the services of which they are the providers.  
They shall provide persons who publish an online public communication service with technical tools enabling them to satisfy the identification conditions laid down in point III.  
A judicial authority may require the service providers mentioned in point I(1) and (2) to communicate the data referred to in the first paragraph.  
The provisions of Articles 226-17, 226-21 and 226-22 of the Criminal Code shall apply to the processing of those data.  
A decree to be adopted following consultation of the Conseil d’État (Council of State) and after consultation of the Data Protection Authority shall define the data referred to in the first paragraph and determine the period for which, and the methods by which, those data is to be retained.  
…’  
   
The CMF  
24      The first paragraph of Article L. 621-10 of the Code monétaire et financier (Monetary and Financial Code), in the version applicable to the disputes in the main proceedings (‘the CMF’), provided:  
‘Investigators and reviewers may, for the purposes of their investigation or review, be provided with all documents, whatever their format. Investigators may also be provided with the data retained and processed by telecommunications operators in the context of Article L. 34-1 of [the CPCE] and the service providers referred to in point I(1) and (2) of Article 6 of the [LCEN] and obtain copies of those data.  
…’  
25      After drawing conclusions from the decision of 21 July 2017 of the Conseil constitutionnel (Constitutional Council, France) declaring unconstitutional the second sentence of the first paragraph of Article L. 621-10 of the CMF, the legislature, by loi no 2018-898, du 23 octobre 2018, relative à la lutte contre la fraude (Law No 2018-898 of 23 October 2018 on combating fraud) (JORF of 24 October 2018, text No 1), inserted Article L. 621-10-2 into the Code monétaire et financier (Monetary and Financial Code), which provides:  
‘For the purpose of investigating market abuse as defined by Regulation [No 596/2014], the investigators may be provided with the data retained and processed by telecommunications operators, subject to the conditions and within the limits laid down in Article L. 34-1 of the [CPCE], and by the service providers referred to in point I(1) and (2) of Article 6 of the [LCEN].  
Communication of the data mentioned in the first paragraph of this Article shall be the subject of prior authorisation by a reviewer of connection data requests.  
The reviewer of connection data requests shall be, alternately, either an active or honorary member of the Conseil d’État (Council of State) elected by the General Assembly of the Conseil d’État (Council of State), then either an active or honorary judge of the Cour de cassation (Court of Cassation, France) elected by the General Assembly of that court. His or her alternate, from the other court, shall be appointed in accordance with the same rules. The reviewer of connection data requests and his or her alternate shall be elected for a non-renewable four-year term.  
…  
The reviewer of connection data requests may not receive or request any instruction from the Autorité des marchés financiers (Financial Markets Authority, France) or from any other authority in the performance of his or her duties. He or she shall be bound by the obligation of professional secrecy subject to the conditions laid down in Article L. 621-4 of this Code.   
The matter shall be referred to him or her by reasoned request from the Secretary General or Deputy Secretary General of the Autorité des marchés financiers (Financial Markets Authority). The request shall contain information justifying its substance.   
The authorisation shall be included in the investigation file.   
The investigators shall use the data submitted by the telecommunications operators and service providers referred to in the first paragraph of this Article exclusively for the purposes of the investigation in the context of which they received the authorisation.  
Connection data relating to acts which are the subject of notifications of objections by the Board of the Autorité des marchés financiers (Financial Markets Authority) shall be destroyed after a period of six months from the final decision of the Enforcement Committee or the appeal courts. In the case of an administrative settlement, the six-month period shall run from the date of execution of the agreement.  
Connection data relating to acts which have not been the subject of a notification of objections by the Board of the Autorité des marchés financiers (Financial Markets Authority) shall be destroyed after a period of one month from the date of the decision of the Board.  
In the event that the investigation report is sent to the procureur de la République financier (Financial Public Prosecutor, France) or the procureur de la République financier (Financial Public Prosecutor) brings a public prosecution ..., the connection data shall be delivered to the procureur de la République financier (Financial Public Prosecutor) and shall not be retained by the Autorité des marchés financiers (Financial Markets Authority).  
The detailed rules for the implementation of this Article shall be set out in a decree to be adopted following consultation of the Conseil d’État (Council of State).’  
   
The disputes in the main proceedings, the questions referred for a preliminary ruling and the procedure before the Court  
26      Further to an application made by the public prosecutor on 22 May 2014, a judicial investigation was launched into VD and SR in respect of acts constituting the offences of insider dealing and concealment of insider dealing. That investigation was subsequently extended, by a first supplementary application of 14 November 2014, to cover the offence of aiding and abetting.   
27      On 23 and 25 September 2015, the Autorité des marchés financiers (Financial Markets Authority; ‘AMF’) sent to the investigating judge certain information available to it in the context of an investigation which it had carried out under Article L. 621-10 of the CMF, which included personal data from telephone calls made by VD and SR which the AMF investigators had collected, on the basis of Article L. 34-1 of the CPCE, from operators providing electronic communications services.   
28      Further to that report issued by the AMF, the investigation was extended, by three supplementary applications of 29 September 2015, 22 December 2015 and 23 November 2016, to cover the offences of corruption and money laundering.   
29      On 10 March and 29 May 2017 respectively, VD and SR were placed under investigation; the investigation in respect of VR related to the offences of insider dealing and money laundering, while the investigation in respect of SR related to the offence of insider dealing.   
30      In so far as the investigation into them was based on the traffic data provided by the AMF, VD and SR each brought an action before the cour d’appel de Paris (Court of Appeal, Paris, France), relying, inter alia, on a plea alleging, in essence, infringement of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter. Specifically, VD and SR, relying on the case-law arising from the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), challenged the fact that that authority took Article L. 621-10 of the CMF and Article L. 34-1 of the CPCE as its legal basis for the collection of those data, while those provisions, first, did not comply with EU law in so far as they provided for general and indiscriminate retention of connection data and, second, laid down no restrictions on the powers of the AMF’s investigators to require the retained data to be provided to them.   
31      By two judgments of the cour d’appel de Paris (Court of Appeal, Paris) of 20 December 2018 and 7 March 2019, that court rejected the action brought by VD and SR. It is apparent from the information in the requests for a preliminary ruling that, when it rejected the plea alleging, in essence, infringement of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, the court adjudicating on the substance of the case relied, inter alia, on the fact that Article 23(2)(h) of Regulation No 596/2014, relating to market abuse, allows the competent authorities to require, in so far as permitted by national law, existing data traffic records held by operators providing electronic communications services, where there is a reasonable suspicion of an infringement of the prohibition on insider dealing under Article 14(a) and (b) of that regulation and where such records may be relevant to the investigation of that infringement.   
32      VD and SR brought an appeal against those judgments before the referring court, raising a plea alleging infringement, inter alia, of the provisions of the Charter and Directive 2002/58 referred to in the preceding paragraph.  
33      As regards access to the connection data, the referring court refers to a decision of the Conseil constitutionnel (Constitutional Council, France) of 21 July 2017, from which it is apparent that the procedure for accessing personal data retained by the AMF investigators, as provided for by French law, is not consistent with the right to respect for privacy, as protected by Article 2 of the Declaration of the Rights of Man and of the Citizen of 1789, stating that, although the national legislature had given authorised agents who are obliged to observe professional secrecy the power to obtain such data in the context of an investigation and had not given them enforcement powers, it had not, however, built into that procedure any other guarantee such as to ensure an equal balance between, first, the right of respect for privacy and, second, the prevention of breaches of public order and the investigation of offenders, with the result that the second sentence of the first paragraph of Article L. 621-10 of the CMF had to be declared to be contrary to the French Constitution.  
34      The referring court also notes, first, that the Conseil constitutionnel (Constitutional Council) took the view that, in view of the ‘manifestly excessive’ consequences that immediate repeal of that provision might have for pending proceedings, it was necessary to defer the date of that repeal to 31 December 2018 and, second, that the national legislature, drawing the appropriate conclusions from the declaration that the first paragraph of Article L. 621-10 of the CMF was unconstitutional, inserted Article L. 621-10-2 into that code.  
35      The referring court, while recalling the findings set out in paragraph 125 of the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), is of the opinion that, in view of the fact that the effects of the repeal of the second sentence of the first paragraph of Article L. 621-10 of the CMF, applicable at the material time, were postponed, it cannot result from the declaration that that provision is unconstitutional that it is invalid. It takes the view, however, that the power of AMF investigators under that provision to obtain connection data without prior review by a court or an independent administrative authority is inconsistent with the requirements of Articles 7, 8 and 11 of the Charter, as interpreted by the Court.   
36      In those circumstances, the only question that arises in that regard is whether it is possible to postpone the temporal effects of the repeal of Article L. 621-10 of the CMF, even though it does not comply with the Charter.   
37      As regards the retention of connection data, the referring court states first of all that, although point II of Article L. 34-1 of the CPCE lays down an obligation in principle, according to which operators providing electronic communications services must erase or make anonymous any traffic data, that obligation is nevertheless accompanied by a number of exceptions, including the exception laid down in point III of that provision, relating to ‘the purposes of investigating, detecting and prosecuting criminal offences’. For those specific purposes, the operations to erase or make anonymous certain pieces of data would be deferred for one year.   
38      It states, in that regard, that the five categories of data concerned in particular by the conditions laid down in point III of Article L. 34-1 of the CPCE are those set out in Article R. 10-13 of the CPCE. Those connection data are generated or processed following a communication and relate to the circumstances of that communication and service users, but give no indication of the content of the communications concerned.  
39      Next, the referring court makes reference to paragraph 112 of the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), according to which Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and observes that, in the context of the cases in the main proceedings, the AMF had access to the data retained by operators providing electronic communications services as there were suspicions concerning insider dealing and market abuse that may fall within the scope of a number of serious offences. That access was justified by the need for that authority, in order to ensure the effectiveness of its investigation, to cross-reference various pieces of retained data over a certain period of time, with a view to updating the inside information being exchanged by a number of interlocutors, which revealed the existence of unlawful practices in that regard.  
40      According to the referring court, the investigations carried out by the AMF satisfy the obligations imposed on the Member States by Article 12(2)(d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, read in the light of Article 1 of that regulation, including, in particular, the obligation to require existing data traffic records held by operators providing electronic communications services to be submitted.   
41      In addition, that court, first, refers to recital 65 of that regulation and observes that those connection data constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing since they make it possible to establish the identity of a person responsible for the dissemination of false or misleading information or that persons have been in contact at a certain time.   
42      Second, the referring court cites recital 66 of that regulation, from which it is apparent that the exercise of powers conferred on competent authorities in the field of finance may interfere with the right to respect for private and family life, home and communications and that, consequently, Member States should have in place adequate and effective safeguards against any abuse by restricting the scope of those powers solely to where they are necessary for the proper investigation of serious cases where there are no equivalent means for effectively achieving the same result. According to that court, it follows from that recital that certain cases of market abuse must be regarded as serious infringements.  
43      The referring court also observes that, in the cases in the main proceedings, the inside information that may have constituted the substantive element of the unlawful market practices was essentially oral information that was secret.  
44      In the light of the findings above, the referring court is uncertain how to reconcile Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter with the requirements under Article 12(2)(d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014.   
45      Lastly, should the Court find that the legislation on the retention of the connection data at issue in the main proceedings does not comply with EU law, the question arises as to whether that legislation retains its effects provisionally, in order to avoid legal uncertainty and to allow the data previously collected and retained to be used for the purpose of detecting insider dealing and bringing criminal proceedings in respect of it.  
46      In those circumstances, the Cour de cassation (Court of Cassation) decided to stay the proceedings and to refer the following questions, which are worded identically in Cases C-399/20 and C-397/20, to the Court of Justice for a preliminary ruling:  
‘(1)      Do Article 12(2)(a) and (d) of Directive [2003/6] and Article 23(2)(g) and (h) of Regulation [No 596/2014], which replaced that directive from 3 July 2016, read in the light of recital 65 of that regulation, not imply that, account being taken of the covert nature of the information exchanged and the fact that the potential subjects of investigation are members of the general public, the national legislature must be able to require electronic communications operators to retain connection data on a temporary but general basis in order to enable the administrative authority referred to in Article 11 of [Directive 2003/6] and Article 22 of [Regulation No 596/2014], in the event of the emergence of grounds for suspecting certain persons of being involved in insider dealing or market manipulation, to require the operator to surrender existing records of traffic data in cases where there are reasons to suspect that the records so linked to the subject matter of the investigation may prove relevant to the production of evidence of the actual commission of the breach, to the extent, in particular, that they offer a means of tracing the contacts established by the persons concerned before the suspicions emerged?  
(2)      If the answer … [to the first question] is such as to prompt the Cour de cassation (Court of Cassation) to form the view that the French legislation on the retention of connection data is not consistent with EU law, could the effects of that legislation be temporarily maintained in order to avoid legal uncertainty and to enable data previously collected and retained to be used for one of the objectives of that legislation?  
(3)      May a national court temporarily maintain the effects of legislation enabling the officials of an independent administrative authority responsible for investigating market abuse to obtain access to obtain connection data without prior review by a court or another independent administrative authority?’  
47      By decision of the President of the Court of 17 September 2020, Cases C-339/20 and C-397/20 were joined for the purposes of the written and oral parts of the procedure and of the judgment.  
48      On 21 April 2021, the Conseil d’État (Council of State, France) delivered the judgment in   
French Data Network and Others  
 (No 393099, 394922, 397844, 397851, 424717, 424718), by which it ruled, inter alia, on the compatibility with EU law of certain national legislative provisions which are relevant to the disputes in the main proceedings, namely Article L. 34-1 of the CPCE and Article R. 10-13 of the CPCE.  
49      At the Court’s invitation, the participants in the hearings in the present cases were given the opportunity to express their views on the effect, if any, of that judgment of the Conseil d’État (Council of State) on the present references for a preliminary ruling.  
50      The representative of the French Government stated at that hearing that, by that judgment, the Conseil d’État (Council of State), in essence, declared unlawful the provisions implementing the general and indiscriminate retention of connection data for the purposes of fighting crime with the exception of the retention of IP addresses and data relating to the civil identity of users of electronic communications networks, thereby giving due effect to the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791). He stated, however, that, in the context of the proceedings, the Conseil d’État (Council of State) also had to respond to the French Government’s objection that that interpretation of EU law was inconsistent with rules of constitutional status, namely those relating to the prevention of breaches of public order, in particular the safety of persons and property, and the investigation of offenders.  
51      In that regard, the representative of the French Government explained that the Conseil d’État (Council of State) had rejected that objection in two stages. First, it is true that it acknowledged that the general and indiscriminate retention of the connection data was a decisive factor for the success of criminal investigations and that no other method could effectively take the place of those investigations. Second, however, the Conseil d’État (Council of State) relied, in particular, on paragraph 164 of the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and took the view that the expedited retention of data was authorised by EU law including where that expedited retention related to data initially retained for the purpose of safeguarding national security.   
52      Furthermore, the representative of the French Government noted that, following the judgment of the Conseil d’État (Council of State) of 21 April 2021,   
French Data Network and Others  
 (No 393099, 394922, 397844, 397851, 424717 and 424718), the national legislature had inserted point III bis into Article L. 34-1 of the Post and Electronic Communications Code, as mentioned in paragraph 21 of the present judgment.  
   
Consideration of the questions referred  
   
Preliminary observations   
53      In the first place, it should be noted that, after the present requests for a preliminary ruling had been lodged, the Conseil d’État (Council of State) delivered the judgment of 21 April 2021,   
French Data Network and Others  
 (No 393099, 394922, 397844, 397851, 424717, 424718), concerning, inter alia, the compatibility with EU law of Article L. 34-1 of the CPCE and Article R. 10-13 of the CPCE.   
54      As the Advocate General observed in point 42 of his Opinion, and as is also apparent from the explanations provided by the referring court, as set out in paragraphs 27, 37 and 38 above, those articles are ‘key provisions’ in the context of the application of Article L. 621-10 of the CMF, which is at issue in the main proceedings.   
55      At the hearing before the Court, after highlighting the legislative development of Article L. 34-1 of the CPCE in response to the clarifications provided by the Court in the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), as referred to in paragraph 21 of the present judgment, the representative of the French Government indicated, in essence, that, in order to resolve the disputes in the main proceedings, the referring court was required, in accordance with the principle of the application of the law   
ratione temporis  
 enshrined in Article 7 and 8 of the Declaration of the Rights of Man and of the Citizen of 1789, to take account of provisions of national law in the version applicable to the facts at issue in the main proceedings, which date from 2014 and 2015, with the result that the judgment of the Conseil d’État (Council of State) of 21 April 2021,   
French Data Network and Others   
(No 393099, 394922, 397844, 397851, 424717, 424718) could not be taken into consideration in any event when analysing the present requests for a preliminary ruling  
.   
56      According to settled case-law, in proceedings under Article 267 TFEU, it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine in the light of the particular circumstances of the case both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions submitted by the national court concern the interpretation of Union law, the Court of Justice is, in principle, bound to give a ruling (see, to that effect, judgment of 8 September 2010,   
Winner Wetten  
, C-409/06, EU:C:2010:503, paragraph 36 and the case-law cited).  
57      The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see, to that effect, judgment of 19 November 2009,   
Filipiak  
, C-314/08, EU:C:2009:719, paragraph 42 and the case-law cited).  
58      In the present case, it is apparent from the orders for reference that the first and third questions directly concern, not Article L. 34-1 of the CPCE and Article R. 10-13 of the CPCE, but Article L. 621-10 of the CMF, pursuant to which the AMF asked operators providing electronic communications services to submit to it traffic data relating to telephone calls made by VD and SR, on the basis of which an investigation was opened into them and the admissibility of which as evidence is disputed in the main proceedings.   
59      In addition, it should be noted that, by the second and third questions referred in the present cases, which are an extension of the first questions, the referring court asks, in essence, whether, in the event that the national legislation at issue relating to the retention of and access to connection data proves to be incompatible with EU law, its effects could not, nevertheless, be provisionally maintained, so as to avoid legal uncertainty and to allow the data retained on the basis of that legislation to be used for the purposes of detecting insider dealing and bringing prosecutions accordingly.   
60      In the light of the considerations above, as well as those referred to by the Advocate General in points 44 to 47 of his Opinion, it must be held that, irrespective of the judgment of the Conseil d’État (Council of State) of 21 April 2021,   
French Data Network and Others  
 (No 393099, 394922, 397844, 397851, 424717, 424718), and of the decision of the Conseil constitutionnel (Constitutional Council) of 25 February 2022 (No 2021-976/977), which declared Article L. 34-1 of the CPCE, in the version referred to in paragraph 20 of the present judgment, to be unconstitutional in part, an answer from the Court to the questions referred remains necessary in order to resolve the disputes in the main proceedings.  
61      In the second place, it should be noted that, at the hearing before the Court, VD’s representative disputed the applicability   
ratione temporis  
 of Regulation No 596/2014, claiming, in essence, that the facts at issue in the main proceedings had occurred before the entry into force of that regulation. Therefore, only the provisions of Directive 2003/6 are relevant for the purposes of examining the questions referred by the national court.  
62      In that regard, it must be borne in mind that, according to settled case-law, a new rule of law applies from the entry into force of the act introducing it, and, while it does not apply to legal situations that have arisen and become final under the old law, it does apply to their future effects, and to new legal situations. The position is otherwise, subject to the principle of the non-retroactivity of legal acts, only if the new rule is accompanied by special provisions which specifically lay down its conditions of temporal application (see, to that effect, judgments of 15 January 2019,   
E.B  
., C-258/17, EU:C:2019:17, paragraph 50 and the case-law cited, and of 14 May 2020,   
Azienda Municipale Ambiente  
, C-15/19, EU:C:2020:371, paragraph 57).  
63      As has been pointed out in paragraphs 26 to 29 above, although the legal situations concerned by the cases in the main proceedings arose before the entry into force of Regulation No 596/2014, which repealed and replaced Directive 2003/6 with effect from 3 July 2016, the proceedings in the main proceedings continued after that date, with the result that, as from that date, the future effects of those situations are, in accordance with the principle recalled in the preceding paragraph, governed by Regulation No 596/2014.  
64      It follows that the provisions of Regulation No 596/2014 are applicable in the present case. Moreover, there is no need to draw a distinction between the provisions referred to by the referring court resulting from Directive 2003/6 and Regulation No 596/2014, since their scope is essentially similar for the purposes of the interpretation which the Court will be required to give in the present cases.  
   
The first question  
   
65      By its first question, the referring court asks, in essence, whether Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, read in conjunction with Article 15(1) of Directive 2002/58, and in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures such as the one at issue in the main proceedings which, as a preventive measure, in order to combat market abuse offences including insider dealing, provide for the general and indiscriminate retention of traffic data for a year from the date on which they were recorded.  
66      The parties to the main proceedings and the interested parties that submitted written observations to the Court have expressed differing views in that regard. For the Estonian Government, for Ireland and for the Spanish and French Governments, Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014 implicitly but necessarily empower the national legislature to impose a general and indiscriminate obligation on operators providing electronic communications services to retain data in order to allow the competent financial authority to detect and impose sanctions for insider dealing. Since, as is apparent from recital 65 of Regulation No 596/2014, those records constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing, such an obligation to retain is necessary both for ensuring the efficacy of instigations led by and prosecutions brought by that authority and, at the same time, the effectiveness of Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(h) of Regulation No 596/2014, and in order to meet the general interest objectives pursued by those instruments, which seek to guarantee the integrity of the EU financial markets and to enhance investor confidence in those markets.  
67      VD, SR, the Polish Government and the European Commission submit, on the other hand, that those provisions, in so far as they merely provide a framework for the power to require operators providing electronic communications services to send ‘existing’ traffic data records held by those operators, govern only the issue of access to those data.  
68      In that regard, it should be noted, in the first place, that it is settled case-law that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation (see, to that effect, judgment of 17 April 2018,   
Egenberger  
, C-414/16, EU:C:2018:257, paragraph 44).  
69      As regards the wording of the provisions referred to in the first question, it should be noted that, while Article 12(2)(d) of Directive 2003/6 refers to the power of the competent financial authority to ‘require existing telephone and existing data traffic records’, Article 23(2)(g) and (h) of Regulation No 596/2014 refers to the power of that authority to require, first, ‘existing … data traffic records held by investment firms, credit institutions or financial institutions’ and, second, to require, ‘in so far as permitted by national law, existing data traffic records held by a telecommunications operator’.   
70      It is clear from the wording of those provisions that they merely provide a framework for that authority’s power to ‘require’ the data available to those operators, which corresponds to access to those data. Furthermore, the reference made to ‘existing’ records, such as those ‘held’ by those operators, suggests that the EU legislature did not intend to lay down rules governing the option open to the national legislature to impose an obligation to retain such records.  
71      In that regard, in accordance with settled case-law, an interpretation of a provision of EU law cannot have the result of depriving the clear and precise wording of that provision of all effectiveness. Thus, where the meaning of a provision of EU law is absolutely plain from its very wording, the Court cannot depart from that interpretation (judgment of 25 January 2022,   
VYSOČINA WIND  
, C-181/20, EU:C:2022:51, paragraph 39 and the case-law cited).  
72      The interpretation outlined in paragraph 70 above is supported both by the context of Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, and by the objectives pursued by the rules of which those provisions form part.  
73      As regards the context of those provisions, it should be noted that, although, under Article 12(1) of Directive 2003/6 and Article 23(3) of Regulation No 596/2014, read in the light of recital 62 of that regulation, the EU legislature intended to require the Member States to take the necessary measures to ensure that the competent financial authorities have a set of effective tools, powers and resources as well as the necessary supervisory and investigatory powers to ensure the effectiveness of their duties, those provisions make no mention of any option open to Member States of imposing, for that purpose, an obligation on operators providing electronic communications services to retain generally and indiscriminately traffic data, nor do they set out the conditions in which those data must be retained by those operators so that they can be submitted to the competent authorities where appropriate.   
74      By Article 12(2) of Directive 2003/6 and Article 23(2) of Regulation No 596/2014, the EU legislature merely intended to grant to the competent financial authority, in order to ensure the effectiveness of its investigative and supervisory duties, ordinary powers of investigation, such as those enabling that authority to have access to documents, to carry out inspections and searches, or to issue orders or prohibitions against persons suspected of having committed market abuse offences including, inter alia, insider dealing.   
75      Furthermore, it is clear that the provisions of Regulation No 596/2014 which specifically govern the question of data retention, namely the final subparagraph of Article 11(5), the second subparagraph of Article 11(6), Article 11(8), Article 11(11)(c), the first subparagraph of Article 17(1), Article 18(5) and Article 28 of that regulation, impose such an obligation to retain only on financial operators, as listed in Article 23(2)(g) of that regulation, and therefore concern only data relating to financial transactions and services provided by those specific operators.  
76      As regards the objectives pursued by the legislation at issue, it must be observed that it is apparent, first, from recitals 2 and 12 of Directive 2003/6 and, second, from Article 1 of Regulation No 596/2014, read in the light of recitals 2 and 24 thereof, that the purpose of those instruments is to protect the integrity of EU financial markets and to enhance investor confidence in those markets, a confidence which depends, inter alia, on investors being placed on an equal footing and being protected against the improper use of inside information. The purpose of the prohibition on insider dealing laid down in Article 2(1) of Directive 2003/6 and Article 8(1) of Regulation No 596/2014 is to ensure equality between the contracting parties in stock-market transactions by preventing one of them who possesses inside information and who is, therefore, in an advantageous position vis-à-vis other investors, from profiting from that information, to the detriment of those who are unaware of it (see, to that effect, judgment of 15 March 2022,   
Autorité des marchés financiers  
, C-302/20, EU:C:2022:190, paragraphs 43, 65 and 77 and the case-law cited).  
   
77      Although, according to recital 65 of Regulation No 596/2014, connection data records constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing and market manipulation, the fact remains that that recital makes reference only to records ‘held’ by operators providing electronic communications services and to the power of that competent financial authority to ‘require’ those operators to send ‘existing’ data. Thus, it is in no way apparent from that recital that the EU legislature intended, by that regulation, to give Member States the power to impose on operators providing electronic communications services a general obligation to retain data.  
78      In the light of the foregoing, it must be held that neither Directive 2003/6 nor Regulation No 596/2014 can be interpreted as capable of constituting the legal basis for a general obligation to retain the data traffic records held by operators providing electronic communications services for the purposes of exercising the powers conferred on the competent financial authority under Directive 2003/6 and Regulation No 596/2014.  
79      In the second place, it should be borne in mind that, as the Advocate General noted, in essence, in points 53 and 61 of his Opinion, Directive 2002/58 is the measure of reference on the retention and, more generally, the processing of personal data in the electronic communications sector, which means that the Court’s interpretation in the light of that directive also governs the traffic data records held by operators providing electronic communications services, which the competent financial authorities, within the meaning of Article 11 of Directive 2003/6 and Article 22 of Regulation No 596/2014, may require from those operators.  
80      According to Article 1(1) of Directive 2002/58, that directive provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector, the latter of which also covers the telecommunications sector.  
81      Moreover, it is apparent from Article 3 of that directive that it is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices. Consequently, that directive must be regarded as regulating the activities of the providers of such services, including, in particular, telecommunications operators (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 93 and the case-law cited).  
82      In the light of the foregoing, it must be held that, as the Advocate General submits, in essence, in points 62 and 63 of his Opinion, the assessment of the lawfulness of the processing of records held by operators providing electronic communications services, as provided for in Article 12(2)(d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, must be carried out in the light of the conditions laid down by Directive 2002/58 and of the interpretation of that directive in the Court’s case-law.  
83      That interpretation is borne out by Article 3(1)(27) of Regulation No 596/2014, in that it provides that, for the purposes of that regulation, traffic data records are those defined in point (b) of the second paragraph of Article 2 of Directive 2002/58.  
84      In addition, according to recital 44 of Directive 2003/6 and recitals 66 and 77 of Regulation No 596/2014, the purposes of those instruments are to pursue the fundamental rights and principles enshrined in the Charter, including the right to privacy. In that regard, the EU legislature expressly stated in recital 66 of Regulation No 596/2014 that, for the purposes of exercising the powers conferred on the competent financial authority under that regulation, which may amount to serious interferences with the right to respect for private and family life, home and communications, Member States should have in place adequate and effective safeguards against any abuse, for instance, where appropriate a requirement to obtain prior authorisation from the judicial authorities of a Member State concerned. Member States should make provision for the competent authorities to exercise such intrusive powers only to the extent that they are necessary for the proper conduct of an investigation into serious cases where there are no equivalent means for effectively arriving at the same result. It follows that the application of the measures governed by Directive 2003/6 and by Regulation No 596/2014 cannot, in any event, undermine the protection of personal data conferred under Directive 2002/58 (see, by analogy, judgment of 29 January 2008,   
Promusicae  
, C-275/06, EU:C:2008:54, paragraph 57, and of 17 June 2021,   
M.I.C.M.  
, C-597/19, EU:C:2021:492, paragraph 124 and the case-law cited).  
85      Consequently, Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014 must be interpreted as not authorising the general and indiscriminate retention of traffic and location data for the purpose of combating market abuse offences and, in particular, insider dealing, since the compatibility with EU law of provisions of national law providing for such retention must be assessed in the light of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted in the Court’s case-law.  
86      As regards the examination of whether such national legislation is compatible with those provisions, it must be borne in mind that, as is apparent, in essence, from a combined reading of paragraphs 53, 54 and 58 of the present judgment, although the provision at the heart of the present references for a preliminary ruling is Article L. 621-10 of the CMF, under which the AMF requested operators providing electronic communications services to transmit traffic data relating to telephone calls made by VD and SR, on the basis of which an investigation was opened into the latter, the fact remains that, as the Advocate General noted in point 42 of his Opinion, Article 34-1 of the CPCE and Article R. 10-13 of the CPCE are ‘key provisions’ for the application of Article L. 621-10 of the CMF.   
87      It is apparent from the explanations provided by the referring court, as summarised in paragraphs 27, 37 and 38 of the present judgment, that, first, the AMF investigators had collected the traffic data at issue on the basis of Article L. 34-1 of the CPCE, in the version applicable to the disputes in the main proceedings, point III of which established a certain number of exceptions to the obligation in principle laid down in point II of that article, according to which operators providing electronic communications services had to erase or make anonymous any traffic data, one exception of which related to ‘the purposes of investigating, detecting and prosecuting criminal offences’. For those specific purposes, operations for the erasing or making anonymous of certain types of data were deferred for one year.  
88      Second, that court states that the five categories of data concerned by point III of Article L. 34-1 of the CPCE, in the version applicable to the disputes in the main proceedings, were those listed in Article R. 10-13 of the CPCE, namely (i) information identifying the user, (ii) data relating to the communications terminal equipment used, (iii) the technical characteristics and date, time and duration of each communication, (iv) data relating to the additional services requested or used and the providers of those services and (v) data identifying the addressee or addressees of the communication. It is also clear from point II of Article R. 10-13 of the CPCE, in the version applicable to the main proceedings, that, in the case of telephony activities, the operators concerned could also retain data enabling the origin and location of the communication to be identified.  
89      It follows that the legislation at issue in the main proceedings covers all means of telephone communications and applies to all users of such means, without distinction or exception. Furthermore, the data which must be retained by operators providing electronic communications services under that legislation are, in particular, the data necessary for locating the source of a communication and its destination, for determining the date, time, duration and type of communication, for identifying the communications equipment used, and for locating the terminal equipment and communications, data which comprise, inter alia, the name and address of the user, the telephone numbers of the caller and the person called.   
90      Thus, although the data which must, under the national legislation at issue, be retained for a period of one year do not cover the content of the communications concerned, they make it possible, inter alia, to identify the person with whom the user of a means of telephone communication has communicated and how, to determine the date, time and duration of the communications and the place from which those communications and connections took place, and to ascertain the location of the terminal equipment without any communication necessarily having been transmitted. In addition, those data enable the frequency of a user’s communications with certain persons over a given period of time to be established. Therefore, it is necessary to take the view that those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, those data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 45 and the case-law cited).  
91      As regards the objectives pursued, the purpose of the legislation at issue is, inter alia, the investigation, detection and prosecution of criminal offences, including those relating to market abuse such as insider dealing.   
92      In the light of the factors set out in paragraphs 86 to 91 above, it must be held that, for the purposes, inter alia, of the investigation, detection and prosecution of criminal offences and the fight against crime, the national legislature provided, by the legislation at issue, for the general and indiscriminate retention of traffic data for one year from the day on which it was recorded.  
93      It is apparent, in particular, from paragraphs 140 to 168 of the judgment of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and from paragraphs 59 to 101 of the judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
 (C-140/20, EU:C:2022:258), that such retention cannot be justified by such objectives under Article 15(1) of Directive 2002/58.   
94      It follows that national legislation, such as that at issue in the main proceedings, which requires operators providing electronic communications services, as a preventive measure, in order to combat market abuse offences including insider dealing, to retain generally and indiscriminately the traffic data of all users of means of electronic communication, with no differentiation in that regard or with no provision made for exceptions and without establishing the link required, in accordance with the case-law referred to in the previous paragraph, between the data to be retained and the objective pursued, falls outside of what is strictly necessary and cannot be considered to be justified, in a democratic society, as is required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (see, to that effect, judgment of 6 October 2020,   
Privacy International  
, C-623/17, EU:C:2020:790, paragraph 81).  
95      In the light of the foregoing, the answer to the first question in Cases C-339/20 and C-397/20 is that Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014, read in conjunction with Article 15(1) of Directive 2002/58, and in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which, as a preventive measure, in order to combat market abuse offences including insider dealing, provide for the general and indiscriminate retention of traffic data for a year from the date on which they were recorded.  
   
The second and third questions  
96      By its second and third questions in the present cases, which it is appropriate to examine together, the referring court asks, in essence, whether EU law must be interpreted as meaning that a national court may restrict the temporal effects of a declaration of invalidity, under national law, with respect to provisions of national law which, first, require operators providing electronic communications services to retain generally and indiscriminately traffic data and, second, allow such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58 read in the light of the Charter.  
97      At the outset, it should be recalled that the principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State bodies to give full effect to the various provisions of EU law, since the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States. In the light of that principle, where it is unable to interpret national legislation in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 118 and the case-law cited).  
98      Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested. The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 119 and the case-law cited).  
99      It is true that the Court has held, in a case concerning the lawfulness of measures adopted in breach of the obligation under EU law to conduct a prior assessment of the impact of a project on the environment and on a protected site, that if domestic law allows it, a national court may, by way of exception, maintain the effects of such measures where such maintenance is justified by overriding considerations relating to the need to nullify a genuine and serious threat of interruption in the electricity supply in the Member State concerned, which cannot be remedied by any other means or alternatives, particularly in the context of the internal market, and continues only for as long as is strictly necessary to remedy the breach (see, to that effect, judgment of 29 July 2019,   
Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen  
, C-411/17, EU:C:2019:622, paragraphs 175, 176, 179 and 181).  
100    However, unlike a breach of a procedural obligation such as the prior assessment of the impact of a project in the specific field of environmental protection, a failure to comply with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure referred to in the preceding paragraph (see, to that effect, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 121 and the case-law cited).  
101    Maintaining the effects of national legislation such as that at issue in the main proceedings would mean that the legislation would continue to impose on operators providing electronic communications services obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data have been retained (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 122 and the case-law cited).  
102    Therefore, the referring court cannot restrict the temporal effects of a declaration of invalidity which it is bound to make under national law in respect of the national legislation at issue in the main proceedings (see, by analogy, judgment of 5 April 2022,   
Commissioner of An Garda Síochána and Others  
, C-140/20, EU:C:2022:258, paragraph 123 and the case-law cited).  
103    In addition, it should be stated that a temporal restriction of the effects of the interpretation given was not imposed in the judgments of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, EU:C:2016:970), and of 6 October 2020,   
La Quadrature du Net and Others  
 (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), with the result that, in accordance with the case-law recalled in paragraph 98 of this judgment, it should not be imposed in a judgment of the Court subsequent to those judgments.  
104    Lastly, in view of the fact that the referring court is ruling on applications requesting that evidence obtained from traffic data be declared inadmissible on the ground that the national provisions at issue are contrary to EU law, both as regards the retention of data and access to those data, it is necessary to determine the effect of a finding that Article L. 621-10 of the CMF, in the version applicable to the facts at issue in the main proceedings, is incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, on the admissibility of the evidence adduced against VD and SR in the context of the main proceedings.   
105    In that regard, it is sufficient to refer to the Court’s case-law, in particular to the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
 (C-746/18, EU:C:2021:152), from which it follows that such admissibility falls, in accordance with the principle of the procedural autonomy of the Member States, within the scope of national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.  
106    As regards the latter principle, it should be noted that it requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law or by means of access of the competent authority to those data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact (see, to that effect, judgment of 2 March 2021,   
Prokuratuur (Conditions of access to data relating to electronic communications)  
, C-746/18, EU:C:2021:152, paragraph 44 and the case-law cited).  
107    In the light of the findings above, the answer to the second and third questions in the present cases is that EU law must be interpreted as precluding a national court from restricting the temporal effects of a declaration of invalidity which it is required to make, under national law, with respect to provisions of national law which, first, require operators providing electronic communications services to retain generally and indiscriminately traffic data and, second, allow such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of those provisions with Article 15(1) of Directive 2002/58 read in the light of the Charter. The admissibility of evidence obtained pursuant to provisions of national law that are incompatible with EU law is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.  
   
Costs  
108    Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 12(2)(a) and (d) of Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6 and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, read in conjunction with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, and read in the light of Articles 7, 8 and 11 and of Article 52(1) of the Charter of Fundamental Rights of the European Union   
must be interpreted as:  
precluding legislative measures which, as a preventive measure, in order to combat market abuse offences including insider dealing, provide for the general and indiscriminate retention of traffic data for a year from the date on which they were recorded.  
2.        
European Union law must be interpreted as precluding a national court from restricting the temporal effects of a declaration of invalidity which it is required to make, under national law, with respect to provisions of national law which, first, require operators providing electronic communications services to retain generally and indiscriminately traffic data and, second, allow such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of those provisions with Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of the Charter of Fundamental Rights of the European Union. The admissibility of evidence obtained pursuant to provisions of national law that are incompatible with EU law is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

ID: db2a4b4d-2f07-40f8-ad98-71be16acdf00

of 20 Oct 2022, C-77/21 (  
Digi  
)  
General data protection law   
 >   
Chapter II - Principles   
 >   
Purpose limitation   
   
JUDGMENT OF THE COURT (First Chamber)  
20 October 2022 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 5(1)(b) and (e) – Principle of ‘purpose limitation’ – Principle of ‘storage limitation’ – Creation, from an existing database, of a database to carry out tests and correct errors – Further processing of the data – Compatibility of the further processing of those data with the purposes of the initial collection – Retention period in the light of those purposes)  
In Case C-77/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Fővárosi Törvényszék (Budapest High Court, Hungary), made by decision of 21 January 2021, received at the Court on 8 February 2021, in the proceedings  
Digi Távközlési és Szolgáltató Kft.  
v  
Nemzeti Adatvédelmi és Információszabadság Hatóság,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, L. Bay Larsen, Vice-President of the Court, acting as Judge of the First Chamber, P.G. Xuereb, A. Kumin and I. Ziemele (Rapporteur), Judges,  
Advocate General: P. Pikamäe,  
Registrar: I. Illéssy, Administrator,  
having regard to the written procedure and further to the hearing on 17 January 2022,  
after considering the observations submitted on behalf of:  
–        Digi Távközlési és Szolgáltató Kft., by R. Hatala and A.D. László, ügyvédek,  
–        the Nemzeti Adatvédelmi és Információszabadság Hatóság, by G. Barabás, legal adviser, assisted by G.J. Dudás and Á. Hargita, ügyvédek,  
–        the Hungarian Government, by Zs. Biró-Tóth and M.Z. Fehér, acting as Agents,  
–        the Czech Government, by T. Machovičová, M. Smolek and J. Vláčil, acting as Agents,  
–        the Portuguese Government, by P. Barros da Costa, L. Inez Fernandes, I. Oliveira, M.J. Ramos and C. Vieira Guerra, acting as Agents,  
–        the European Commission, by V. Bottka and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 31 March 2022,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 5(1)(b) and (e) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2).  
2        The request has been made in proceedings between Digi Távközlési és Szolgáltató Kft. (‘Digi’), one of the leading internet service and television providers in Hungary, and the Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information, Hungary) (‘the Authority’) regarding a breach of personal data contained in a Digi database.  
   
Legal context  
3        Recitals 10 and 50 of Regulation 2016/679 state:  
‘(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
…  
(50)      The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. … In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.  
…’  
4        Article 4 of Regulation 2016/679, headed ‘Definitions’, provides:  
‘For the purposes of this Regulation:  
…  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…’  
5        Under Article 5 of that regulation, headed ‘Principles relating to processing of personal data’:  
‘1.      Personal data shall be:  
(a)      processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);  
(b)      collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (“purpose limitation”);  
(c)      adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);  
(d)      accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);  
(e)      kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);  
(f)      processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).  
2.      The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’  
6        Article 6 of that regulation, headed ‘Lawfulness of processing’, provides:  
‘1.      Processing shall be lawful only if and to the extent that at least one of the following applies:  
(a)      the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;  
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject;  
(d)      processing is necessary in order to protect the vital interests of the data subject or of another natural person;  
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.  
…  
4.      Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:  
(a)      any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;  
(b)      the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;  
(c)      the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;  
(d)      the possible consequences of the intended further processing for data subjects;  
(e)      the existence of appropriate safeguards, which may include encryption or pseudonymisation.’  
   
Dispute in the main proceedings and the questions referred for a preliminary ruling  
7        Digi is one of the leading internet service and television providers in Hungary.  
8        In April 2018, following a technical failure affecting the operation of a server, Digi created a ‘test’ database (‘the test database’), to which it copied the personal data of around one third of its private customers, which were stored in another database, called the ‘digihu’ database, which could be linked to the website www.digi.hu, containing the up-to-date data of subscribers to Digi’s newsletter, for direct marketing purposes, and the data of systems administrators, giving access to the website interface.  
9        On 23 September 2019, Digi became aware that an ‘ethical hacker’ had gained access to the personal data held by it in relation to around 322 000 persons. Digi was informed of that access by the ‘ethical hacker’ himself, who sent Digi a line from the test database by way of evidence. Digi corrected the fault which had enabled that access and concluded a confidentiality agreement with the hacker, to whom it offered a reward.  
10      After deleting the test database, Digi notified the personal data breach to the Authority on 25 September 2019, and the Authority subsequently opened an investigation.  
11      By decision of 18 May 2020, the Authority found, inter alia, that Digi had infringed Article 5(1)(b) and (e) of Regulation 2016/679, in that, after carrying out the necessary tests and correcting the fault, it had not immediately deleted the test database, with the result that a large amount of personal data had been stored in that database for no purpose for nearly 18 months, in a file from which it was possible for the data subjects to be identified. As a consequence, the Authority required Digi to review all its databases and fined it the sum of 100 000 000 Hungarian forint (HUF) (around EUR 248 000).  
12      Digi challenged the legality of that decision before the referring court.  
13      The referring court points out that the personal data copied by Digi to the test database were collected for the purposes of the conclusion and performance of subscription contracts and that the lawfulness of the initial collection of the personal data was not called into question by the Authority. It wonders, however, whether the effect of the copying, to another database, of the data initially collected was to change the purpose of the initial collection and the processing of those data. It adds that it must also determine whether the creation of a test database and the further processing, in that other database, of customers’ data are compatible with the purposes of the initial collection. It considers that the principle of ‘purpose limitation’, as set out in Article 5(1)(b) of Regulation 2016/679, does not enable it to determine the internal systems in which the controller is entitled to process the lawfully collected data or to ascertain whether the controller may copy those data to a test database without changing the purpose of the initial data collection.  
14      If the creation of the test database is incompatible with the purpose of the initial collection, the referring court also wonders whether, since the purpose of the processing of subscribers’ data in another database was not to correct errors but to conclude contracts, the necessary retention period must, under the principle of ‘storage limitation’ appearing in Article 5(1)(e) of Regulation 2016/679, correspond to the period necessary for the correction of errors or to that necessary for the performance of the contractual obligations.  
15      In those circumstances, the Fővárosi Törvényszék (Budapest High Court, Hungary) decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Must the concept of “purpose limitation” as defined in Article 5(1)(b) of [Regulation 2016/679] … be interpreted as meaning that the fact that the controller stores in parallel in another database personal data which were otherwise collected and stored for a limited legitimate purpose is consistent with that concept or, conversely, is the limited legitimate purpose of collecting those data no longer valid so far as the parallel database is concerned?  
(2)      Should the answer to the first question referred be that the parallel storage of data is in principle incompatible with the principle of “purpose limitation”, is the fact that the controller stores in parallel in another database personal data which were otherwise collected and stored for a limited legitimate purpose compatible with the principle of “storage limitation” established in Article 5(1)(e) of [Regulation 2016/679]?’  
   
Consideration of the questions referred  
   
Admissibility  
16      The Authority and the Hungarian Government expressed doubts as to the admissibility of the questions referred, on the ground that those questions do not correspond to the facts of the dispute in the main proceedings and are not directly relevant to the resolution of that dispute.  
17      In that regard, first, it should be recalled that it follows from settled case-law of the Court that it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions referred concern the interpretation or the validity of a rule of EU law, the Court is in principle bound to give a ruling. It follows that questions referred by national courts enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court only where it appears that the interpretation sought bears no relation to the actual facts of the main action or its object, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 16 July 2020,   
Facebook Ireland and Schrems  
, C-311/18, EU:C:2020:559, paragraph 73 and the case-law cited).  
18      In this case, the referring court has before it an action seeking annulment of a decision penalising Digi, in its capacity as controller, for having breached the principle of ‘purpose limitation’ and the principle of ‘storage limitation’, laid down, respectively, in Article 5(1)(b) and (e) of Regulation 2016/679, by having failed to delete a database containing personal data permitting identification of the data subjects. The questions referred relate precisely to the interpretation of those provisions, with the result that it cannot be found that the interpretation sought of EU law bears no relation to the actual facts of the main action or to its object or is hypothetical. Moreover, the order for reference contains sufficient factual and legal material to give a useful answer to the questions submitted by the referring court.  
19      Secondly, it is important to recall that, in proceedings under Article 267 TFEU, which are based on a clear separation of functions between the national courts and the Court, the national court alone has jurisdiction to interpret and apply national law, while the Court is empowered only to give rulings on the interpretation or the validity of an EU provision on the basis of the facts which the national court puts before it (judgment of 5 May 2022,   
Zagrebačka banka  
, C-567/20, EU:C:2022:352, paragraph 45 and the case-law cited).  
20      Consequently, the argument relating to the inadmissibility of the questions referred, which the Authority and the Hungarian Government base, in essence, on the claim that the questions referred do not correspond to the facts of the dispute in the main proceedings, must be rejected.  
21      It follows that the questions referred are admissible.  
   
Substance  
   
First question  
22      By its first question, the referring court asks, in essence, whether Article 5(1)(b) of Regulation 2016/679 must be interpreted as meaning that the principle of ‘purpose limitation’, laid down in that provision, precludes the recording and storage by the controller, in a database created for the purposes of carrying out tests and correcting errors, of personal data previously collected and stored in another database.  
23      In accordance with settled case-law, the interpretation of a provision of EU law requires account to be taken not only of its wording, but also of its context, and the objectives and purpose pursued by the act of which it forms part (judgment of 1 August 2022,   
HOLD Alapkezelő  
, C-352/20, EU:C:2022:606, paragraph 42 and the case-law cited).  
24      In that regard, in the first place, it should be pointed out that Article 5(1) of Regulation 2016/679 establishes the principles relating to the processing of personal data, which apply to the controller and with which the controller must be able to demonstrate compliance, in accordance with the principle of accountability set out in Article 5(2).  
25      In particular, under Article 5(1)(b) of that regulation, which sets out the principle of ‘purpose limitation’, personal data are, first, to be collected for specified, explicit and legitimate purposes and, second, not to be further processed in a manner that is incompatible with those purposes.  
26      It is thus apparent from the wording of that provision that it comprises two requirements, one relating to the purposes of the initial collection of the personal data and the other concerning the further processing of those data.  
27      Regarding, first, the requirement that personal data are to be collected for specified, explicit and legitimate purposes, it follows from the case-law of the Court that that requirement implies, first of all, that the purposes of the processing are to be identified at the latest at the time of the collection of the personal data, next, that the purposes of that processing are to be clearly stated and, finally, that the purposes of that processing are to guarantee, inter alia, the lawfulness of the processing of those data, within the meaning of Article 6(1) of Regulation 2016/679 (see, to that effect, judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraphs 64 to 66).  
28      In this case, it is apparent from the wording of the first question and the grounds of the order for reference that the personal data at issue in the main proceedings were collected for specified, explicit and legitimate purposes, with the referring court specifying, in addition, that those data were collected for the purposes of the conclusion and performance by Digi of subscription contracts with its customers, in accordance with Article 6(1)(b) of Regulation 2016/679.  
29      With regard, secondly, to the requirement that the personal data are not to be the subject of further processing which is incompatible with those purposes, it should be pointed out, on the one hand, that the recording and storage, by the controller, in a newly created database, of personal data stored in another database constitutes ‘further processing’ of those data.  
30      The concept of ‘processing’ is defined broadly in Article 4(2) of Regulation 2016/679 as covering any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as, inter alia, the collection, recording and storage of those data.  
31      Moreover, in accordance with the usual meaning of the term ‘further’ in everyday language, any processing of personal data which is subsequent to the initial processing constituted by the initial collection of those data constitutes ‘further’ processing of those data, regardless of the purpose of that further processing.  
32      On the other hand, it should be pointed out that Article 5(1)(b) of Regulation 2016/679 does not contain any indication of the circumstances in which further processing of personal data may be regarded as compatible with the purposes of the initial collection of those data.  
33      The context of that provision nevertheless provides, in the second place, useful clarification in that regard.  
34      It is apparent from a combined reading of Article 5(1)(b), Article 6(1)(a) and Article 6(4) of Regulation 2016/679 that the question of the compatibility of the further processing of personal data with the purposes for which those data were initially collected arises only if the purposes of that further processing are not identical to the purposes of the initial collection.  
35      Moreover, it follows from that Article 6(4), read in the light of recital 50 of that regulation, that, where the processing for a purpose other than that for which the data have been collected is not based on the data subject’s consent or on an EU or Member State law, it is necessary, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, to take into account, inter alia, first, any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; secondly, the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; thirdly, the nature of the personal data; fourthly, the possible consequences of the intended further processing for data subjects; and finally, fifthly, the existence of appropriate safeguards in both the original and intended further processing operations.  
36      As the Advocate General noted, in essence, in points 28, 59 and 60 of his Opinion, those criteria reflect the need for a specific, logical and sufficiently close link between the purposes for which the personal data were initially collected and the further processing of those data, and ensure that such further processing does not deviate from the legitimate expectations of the subscribers as to the subsequent use of their data.  
37      Furthermore, in the third place, as the Advocate General emphasised, in essence, in point 27 of his Opinion, those criteria limit the reuse of personal data previously collected by ensuring a balance between, on the one hand, the need for predictability and legal certainty regarding the purposes of the processing of personal data previously collected and, on the other hand, the recognition of a degree of flexibility for the controller in the management of those data, and thereby contribute to the attainment of the objective of ensuring a consistent and high level of protection of natural persons, which is set out in recital 10 of Regulation 2016/679.  
38      Thus, taking into account the criteria mentioned in paragraph 35 of the present judgment and in the light of all of the circumstances characterising the case, it falls to the national court to determine both the purposes of the initial collection of the personal data and those of the further processing of those data and, if the purposes of that further processing are different from the purposes of that collection, to check that the further processing of those data is compatible with the purposes of that initial collection.  
39      That said, it is open to the Court, when giving a preliminary ruling on a reference, to give clarifications to guide the national court in that determination (see, to that effect, judgment of 7 April 2022,   
Fuhrmann-2  
, C-249/21, EU:C:2022:269, paragraph 32).  
40      In this case, first, as was recalled in paragraph 13 of the present judgment, it is apparent from the order for reference that the personal data were initially collected by Digi, the controller, for the purposes of the conclusion and performance of subscription contracts with its private customers.  
41      Second, the parties to the main proceedings are not in agreement on the specific purpose of the recording and storage by Digi, in the test database, of the personal data at issue. While Digi argues that the specific purpose of the creation of the test database was to guarantee access to the subscribers’ data until the errors were corrected, with the result that that purpose was identical to the purposes pursued by the initial collection of those data, the Authority maintains that the specific purpose of the further processing was distinct from those purposes since it was the conducting of tests and the correction of errors.  
42      In that regard, it should be recalled that it is apparent from the case-law cited in paragraph 19 of the present judgment that, in proceedings under Article 267 TFEU, which are based on a clear separation of functions between the national courts and the Court, the national court alone has jurisdiction to interpret and apply national law, while the Court is empowered only to give rulings on the interpretation or the validity of an EU provision on the basis of the facts which the national court puts before it.  
43      It is apparent from the order for reference that the test database was created by Digi in order to be able to carry out tests and correct errors, so that it is in the light of those purposes that it falls to the referring court to assess the compatibility of the further processing with the purposes of the initial collection, being the conclusion and performance of subscription contracts.  
44      Third, regarding that assessment, it should be pointed out that there is a specific link between the conducting of tests and the correction of errors affecting the subscriber database and the performance of the subscription contracts of private customers, in that such errors may be prejudicial to the provision of the contractually agreed service, for which the data were initially collected. As the Advocate General noted in point 60 of his Opinion, such processing does not deviate from the legitimate expectations of those customers as to the subsequent use of their personal data. It is not, furthermore, apparent from the order for reference that those data were sensitive in whole or in part or that the further processing at issue of those data, as such, had detrimental consequences for the subscribers or was not accompanied by appropriate safeguards, which it is, in any event, for the referring court to verify.  
45      It follows from all of the foregoing considerations that the answer to the first question is that Article 5(1)(b) of Regulation 2016/679 must be interpreted as meaning that the principle of ‘purpose limitation’, laid down in that provision, does not preclude the recording and storage by the controller, in a database created for the purposes of carrying out tests and correcting errors, of personal data previously collected and stored in another database, where such further processing is compatible with the specific purposes for which the personal data were initially collected, which must be determined in the light of the criteria in Article 6(4) of that regulation.  
   
Second question  
46      By way of a preliminary point, it should be noted that the referring court’s second question, which relates to the conformity with the principle of ‘storage limitation’, appearing in Article 5(1)(e) of Regulation 2016/679, of the storage by Digi, in the test database, of personal data of its customers, is asked by that court only in the event of the answer to the first question, as reformulated, being in the affirmative, namely if that storage is not compatible with the principle of ‘purpose limitation’, laid down in Article 5(1)(b) of that regulation.  
47      However, first, as the Advocate General noted in point 24 of his Opinion, the principles relating to the processing of personal data set out in Article 5 of Regulation 2016/679 apply cumulatively. Consequently, the storage of personal data must comply not only with the principle of ‘purpose limitation’, but also with that of ‘storage limitation’.  
48      Second, it should be recalled that, as is apparent from recital 10 of Regulation 2016/679, that regulation aims, inter alia, to ensure a high level of protection of natural persons within the European Union and, to that end, to ensure consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of those persons with regard to the processing of personal data throughout the European Union.  
49      To that end, Chapters II and III of that regulation set out, respectively, the principles governing the processing of personal data and the rights of the data subject, which any processing of personal data must observe. In particular, any processing of personal data must, first, comply with the principles relating to the processing of data established in Article 5 of that regulation and, second, in the light, in particular, of the principle of the lawfulness of processing, laid down in Article 5(1)(a), satisfy one of the conditions of the lawfulness of the processing listed in Article 6 of that regulation (see, to that effect, judgments of 22 June 2021,   
Latvijas Republikas Saeima (  
Penalty points  
)  
, C-439/19, EU:C:2021:504, paragraph 96, and of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 50).  
50      In the light of those considerations, even if, formally, the referring court asked the second question only in the event of the answer to the first question, as reformulated, being in the affirmative, that does not prevent the Court from providing the referring court with all the elements of interpretation of EU law which may be of assistance in assessing the case pending before it (see, to that effect, judgment of 17 March 2022,   
Daimler  
, C-232/20, EU:C:2022:196, paragraph 49) and, therefore, from answering the second question.  
51      In those circumstances, it must be found that, by that question, the referring court asks, in essence, whether Article 5(1)(e) of Regulation 2016/679 must be interpreted as meaning that the principle of ‘storage limitation’, laid down in that provision, precludes the storage by the controller, in a database created for the purposes of carrying out tests and correcting errors, of personal data previously collected for other purposes, for longer than is necessary for the conducting of those tests and the correction of those errors.  
52      In the first place, it should be pointed out that, under Article 5(1)(e) of Regulation 2016/679, personal data are to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.  
53      It is thus unequivocally clear from the wording of that article that the principle of ‘storage limitation’ requires the controller to be able to demonstrate, in accordance with the principle of accountability referred to in paragraph 24 of the present judgment, that personal data are kept only for as long as is necessary for the purposes for which they were collected or for which they have been further processed.  
54      It follows that even initially lawful processing of data may over time become incompatible with Regulation 2016/679 where those data are no longer necessary for such purposes (judgment of 24 September 2019,   
GC and Others (De-referencing of sensitive data)  
, C-136/17, EU:C:2019:773, paragraph 74) and that the data must be erased when those purposes have been served (see, to that effect, judgment of 7 May 2009,   
Rijkeboer  
, C-553/07, EU:C:2009:293, paragraph 33).  
55      That interpretation is consistent, in the second place, with the context of Article 5(1)(e) of Regulation 2016/679.  
56      In that regard, it was recalled in paragraph 49 of the present judgment that any processing of personal data must comply with the principles relating to the processing of data set out in Article 5 of that regulation and satisfy one of the conditions relating to the lawfulness of the processing listed in Article 6 of that regulation.  
57      First, as is apparent from such Article 6, where the data subject has not given consent to the processing of his or her personal data for one or more specific purposes, in accordance with Article 6(1)(a) of Regulation 2016/679, the processing must, as is apparent from Article 6(1)(b) to (f), satisfy a requirement of necessity.  
58      Second, such a requirement of necessity follows also from the principle of ‘data minimisation’, laid down in Article 5(1)(c) of that regulation, under which personal data are to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.  
59      Such an interpretation is, in the third place, consistent with the objective pursued by Article 5(1)(e) of Regulation 2016/679, which, as was recalled in paragraph 48 of the present judgment, is, inter alia, to ensure a high level of protection of natural persons within the European Union with regard to the processing of personal data.  
60      In this case, Digi argued that it was due to an oversight that the personal data of a portion of its private customers stored in the test database were not deleted after the tests had been conducted and the errors had been corrected.  
61      In that regard, it is sufficient to point out that that argument is not relevant for the purposes of assessing whether data were kept for longer than was necessary for the purposes for which they were further processed, in breach of the principle of ‘storage limitation’, laid down in Article 5(1)(e) of Regulation 2016/679.  
62      It follows from all of the foregoing considerations that the answer to the second question is that Article 5(1)(e) of Regulation 2016/679 must be interpreted as meaning that the principle of ‘storage limitation’, laid down in that provision, precludes the storage by the controller, in a database created for the purposes of carrying out tests and correcting errors, of personal data previously collected for other purposes, for longer than is necessary for the conducting of those tests and the correction of those errors.  
   
Costs  
63      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
1.        
Article 5(1)(b) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),  
must be interpreted as meaning that the principle of ‘purpose limitation’, laid down in that provision, does not preclude the recording and storage by the controller, in a database created for the purposes of carrying out tests and correcting errors, of personal data previously collected and stored in another database, where such further processing is compatible with the specific purposes for which the personal data were initially collected, which must be determined in the light of the criteria in Article 6(4) of that regulation.  
2.        
Article 5(1)(e) of Regulation 2016/679  
must be interpreted as meaning that the principle of ‘storage limitation’, laid down in that provision, precludes the storage by the controller, in a database created for the purposes of carrying out tests and correcting errors, of personal data previously collected for other purposes, for longer than is necessary for the conducting of those tests and the correction of those errors.

ID: e2913d17-a66a-4866-a3e2-786b0fa2e279

of 26 Oct 2023, C-307/22 (  
FT  
)  
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Transparent information, communication and modalities for the exercise of the rights of the data subject   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
   
JUDGMENT OF THE COURT (First Chamber)  
26 October 2023 (\*)  
(Reference for a preliminary ruling – Processing of personal data – Regulation (EU) 2016/679 – Articles 12, 15 and 23 – Data subject’s right of access to his or her data undergoing processing – Right to obtain a first copy of those data free of charge – Processing of a patient’s data by his or her medical practitioner – Medical records – Reasons for the request for access – Use of data for the purpose of triggering the liability of the person providing treatment – Concept of ‘copy’)  
In Case C-307/22,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 29 March 2022, received at the Court on 10 May 2022, in the proceedings  
FT  
v  
DW,  
THE COURT (First Chamber),  
composed of A. Arabadjiev, President of the Chamber, T. von Danwitz, P.G. Xuereb, A. Kumin and I. Ziemele (Rapporteur), Judges,  
Advocate General: N. Emiliou,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        the Latvian Government, by K. Pommere, acting as Agent,  
–        the European Commission, by A. Bouchagiar, F. Erlbacher and H. Kranenborg, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 20 April 2023,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 12(5), Article 15(3) and Article 23(1)(i) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (‘the GDPR’).  
2        The request has been made in proceedings between FT and DW concerning the refusal by FT, a dentist, to provide her patient with a first copy of his medical records free of charge.  
   
Legal context  
   
European Union law  
3        Under recital 4 of the GDPR:  
‘… The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in [the Charter of Fundamental Rights of the European Union] as enshrined in the Treaties, in particular … freedom to conduct a business …’  
4        Recitals 10 and 11 of the GDPR state:  
‘(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. …  
(11)      Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data …’  
5        Pursuant to recital 13 of the GDPR:  
‘… In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. …’  
6        Recital 58 of the GDPR states:  
‘The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand’.  
7        As is stated in recital 59 of the GDPR:  
‘Modalities should be provided for facilitating the exercise of the data subject’s rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. …’  
8        Recital 63 of the GDPR is worded as follows:  
‘A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided …’  
9        Article 4 of the GDPR provides:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…’  
10      Article 12 of the GDPR provides:  
‘1.      The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.  
2.      The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. …   
…  
5.      Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:  
(a)      charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or  
(b)      refuse to act on the request.  
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.  
…’  
11      Article 15 of the GDPR states:  
‘1.      The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:  
(a)      the purposes of the processing;  
(b)      the categories of personal data concerned;  
(c)      the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;  
(d)      where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;  
(e)      the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;  
(f)      the right to lodge a complaint with a supervisory authority;  
(g)      where the personal data are not collected from the data subject, any available information as to their source;  
(h)      the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.  
2.      Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.  
3.      The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.  
4.      The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.’  
12      Articles 16 and 17 of that regulation enshrine, respectively, the data subject’s right to obtain the rectification of inaccurate personal data (right to rectification) and the right, in certain circumstances, to have those data erased (right to erasure or ‘right to be forgotten’).  
13      Article 18 thereof, entitled ‘Right to restriction of processing’, provides, in paragraph 1 thereof:  
‘The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:  
(a)      the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;  
(b)      the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;  
(c)      the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;  
(d)      the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.’  
14      Article 21 of the GDPR, entitled ‘Right to object’, provides, in paragraph 1 thereof:  
‘The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.’  
15      Under Article 23(1) of the GDPR:  
‘Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
…  
(i)      the protection of the data subject or the rights and freedoms of others;  
…’  
   
German law  
16      According to Paragraph 630f of the Bürgerliches Gesetzbuch (Civil Code; ‘the BGB’), the person providing treatment is obliged to keep medical records in paper form or electronically for the purpose of documentation in direct temporal connection with the treatment. The person providing treatment is obliged to record in the patient’s medical records all measures which, from a professional point of view, are essential for the current and future treatment, and the results of those measures, in particular the patient’s history, diagnoses, examinations, results of examinations, findings, therapies and the effects thereof, procedures and the effects thereof, consents and any explanations given. The person providing treatment must retain the patient’s medical records for a period of 10 years after completion of the treatment, unless other retention periods exist under other provisions.  
17      Under the first sentence of subparagraph 1 of Paragraph 630g of the BGB, upon request, the patient must be granted immediate access to all the medical records concerning him or her, unless such access is precluded by significant treatment-related reasons or other significant rights of third parties. Pursuant to the first sentence of subparagraph 2 of Paragraph 630g of the BGB, the patient may also request electronic copies of his or her medical records. In view of the explanatory memorandum to the law, this must be understood as meaning that the patient may choose to request that either physical or electronic copies be produced. The second sentence of subparagraph 2 of Paragraph 630g of the BGB provides that the patient must reimburse the person providing treatment for the costs incurred.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
18      DW received dental care from FT. Suspecting that errors had been made in the treatment he had been given, DW requested that FT provide, free of charge, a first copy of his medical records. FT informed DW that she would not grant his request unless he agreed to cover the costs connected with providing a copy of the medical records, as is provided for in national law.  
19      DW brought an action against FT. Both at first instance and on appeal, DW’s request to be provided with a first copy of his medical records free of charge was upheld. Those decisions were based on an interpretation of the applicable national legislation in the light of Article 12(5) of the GDPR, as well as Article 15(1) and (3) thereof.  
20      Hearing an appeal on a point of law (  
Revision  
) brought by FT, the Bundesgerichtshof (Federal Court of Justice, Germany) considers that the outcome of the dispute is dependent on the interpretation to be given in respect of the provisions of the GDPR.  
21      The referring court notes that, under national law, the patient may obtain a copy of his or her medical records, provided that he or she reimburses the person providing treatment for the costs resulting therefrom.  
22      However, it could be inferred from the first sentence of Article 15(3) of the GDPR, read in conjunction with the first sentence of Article 12(5) thereof, that the controller – in this instance, the person providing treatment – is required to provide the patient with a first copy of his or her medical records free of charge.  
23      First, the referring court notes that DW is requesting a first copy of his medical records with a view to triggering the liability of FT. Such a purpose is not related to that referred to in recital 63 of the GDPR, which provides for the right to access personal data in order to become aware of the processing of those data and verify the lawfulness of that processing. However, the wording of Article 15 of that regulation does not make exercise of the right to communication subject to the existence of such grounds. In addition, that provision does not require the data subject to provide reasons for his or her request for communication.  
24      Secondly, the referring court emphasises that Article 23(1) of the GDPR permits the adoption of national legislative measures restricting the scope of the obligations and rights provided for in Articles 12 to 22 of that regulation in order to safeguard one of the objectives referred to in that provision. In this instance, FT is relying on the objective of protecting the rights and freedoms of others which is set out in Article 23(1)(i) of the GDPR and argues that the charging system introduced by the second sentence of subparagraph 2 of Paragraph 630g of the BGB is a measure which (i) is necessary and proportionate to safeguard the legitimate interests of persons providing treatment and (ii) as a general rule, contributes to preventing requests for copies by the patients concerned which do not contain a statement of reasons.  
25      However, the second sentence of subparagraph 2 of Paragraph 630g of the BGB was adopted prior to the entry into force of the GDPR.  
26      In addition, the charging system introduced by the second sentence of subparagraph 2 of Paragraph 630g of the BGB is primarily intended to protect the economic interests of persons providing treatment. It is therefore necessary to determine whether the interest of those persons in being relieved of the costs and charges connected with providing copies of data is included in the rights and freedoms of others for the purposes of Article 23(1)(i) of the GDPR. Furthermore, the systematic transfer to patients of the costs connected with copies of their medical records could appear excessive, given that it does not take account either of the amount of costs actually incurred or of the circumstances specific to each request.  
27      Thirdly, in so far as DW is requesting that a copy of all the medical documents concerning him, and thus of all his medical records, be provided, the referring court questions the scope of the right to obtain a copy of personal data undergoing processing, as enshrined in Article 15(3) of the GDPR. In that regard, that right could be complied with through the communication of a summary of the data processed by the medical professional. However, it appears that the objectives of transparency and verifying lawfulness pursued by the GDPR argue in favour of communicating a copy of all the data available to the controller in their original form, namely all the medical documents concerning the patient inasmuch as they contain such data.  
28      In those circumstances the Bundesgerichtshof (Federal Court of Justice) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Must the first sentence of Article 15(3) of [the GDPR], read in conjunction with Article 12(5) thereof, be interpreted as meaning that the controller (in the present case: the doctor providing treatment) is not obliged to provide the data subject (in the present case: the patient), free of charge, with a first copy of his or her personal data processed by the controller where the data subject does not request the copy in order to pursue the purposes referred to in the first sentence of recital 63 of the GDPR, namely to become aware of the processing of his or her personal data and to be able to verify the lawfulness of that processing, but pursues a different purpose – one which is not related to data protection but is legitimate (in the present case: to verify the existence of claims under medical liability law)?  
(2)(a)      If Question 1 is answered in the negative: In accordance with Article 23(1)(i) of the GDPR, can a national provision of a Member State adopted prior to the entry into force of the GDPR also be regarded as a restriction of the right to be provided, free of charge, with a copy of the personal data processed by the controller, as provided for in the first sentence of Article 15(3) of the GDPR, read in conjunction with Article 12(5) thereof?  
(2)(b)      If Question 2(a) is answered in the affirmative: Must Article 23(1)(i) of the GDPR be interpreted as meaning that the rights and freedoms of others, as referred to therein, also include their interest in being relieved of the costs associated with the provision of a copy of data in accordance with the first sentence of Article 15(3) of the GDPR and other expenses incurred in making the copy available?  
(2)(c)      If Question 2(b) is answered in the affirmative: In accordance with Article 23(1)(i) of the GDPR, can national legislation which, in the context of the doctor-patient relationship, provides that the doctor always has a claim for reimbursement of expenses against the patient, irrespective of the specific circumstances of the individual case, where the doctor provides the patient with a copy of the patient’s personal data from the patient’s medical records be regarded as a restriction of the obligations and rights arising from the first sentence of Article 15(3) of the GDPR, read in conjunction with Article 12(5) thereof?  
(3)      If Question 1 is answered in the negative and [Question 2(a), (b) or (c)] is answered in the negative: In the context of the doctor-patient relationship, does the entitlement under the first sentence of Article 15(3) of the GDPR include entitlement to be provided with copies of all parts of the patient’s medical records containing the patient’s personal data, or does it extend only to the provision of a copy of the patient’s personal data as such, with the doctor who processes the data deciding the manner in which he or she compiles the data for the patient concerned?’  
   
Consideration of the questions referred  
   
The first question  
29      By its first question, the referring court asks, in essence, whether Article 12(5) and Article 15(1) and (3) of the GDPR are to be interpreted as meaning that the controller is under an obligation to provide the data subject, free of charge, with a first copy of his or her personal data undergoing processing, even where the reason for that request is not related to those referred to in the first sentence of recital 63 of that regulation.  
30      As a preliminary point, it should be borne in mind that, in accordance with settled case-law, in order to interpret a provision of EU law it is necessary to take account not only of the wording of that provision, but also of its context and the objectives pursued by the rules of which it forms part (judgment of 12 January 2023,   
Österreichische Post (Information regarding the recipients of personal data)  
, C-154/21, EU:C:2023:3, paragraph 29).  
31      Regarding, first, the wording of the relevant provisions, it should be noted that Article 12(5) of the GDPR establishes the principle that the exercise of the data subject’s right of access to his or her data undergoing processing and to the information relating thereto is not to entail any cost for the data subject. Furthermore, that provision envisages two reasons why a controller may either charge a reasonable fee taking into account administrative costs or refuse to act on a request. Those reasons relate to instances of abuses of rights, in which the data subject’s requests are ‘manifestly unfounded’ or ‘excessive’, in particular because of their repetitive character.  
32      In that regard, the referring court has expressly stated that the data subject’s request was not abusive.  
33      In addition, the data subject’s right of access to his or her data undergoing processing and to the information relating thereto, which is an integral part of the right to the protection of personal data, is guaranteed in Article 15(1) of the GDPR. According to the wording of that provision, data subjects have the right to access their personal data undergoing processing.  
34      In addition, it is apparent from Article 15(3) of the GDPR that the controller is to provide a copy of the personal data undergoing processing and that it may charge a reasonable fee for any further copies requested by the data subject. In that regard, Article 15(4) of that regulation specifies that Article 15(3) thereof confers a ‘right’ on that data subject. Such a fee may therefore be charged by the controller only where the data subject has already received, free of charge, a first copy of his or her data and is once again requesting a copy of those data.  
35      As has already been held by the Court, it follows from the literal analysis of the first sentence of Article 15(3) of the GDPR that that provision confers on the data subject the right to obtain a faithful reproduction of his or her personal data, understood in a broad sense, that are subject to operations that can be classified as ‘processing carried out by the controller’ (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 28).  
36      Accordingly, it follows from a combined reading of Article 12(5) of the GDPR and Article 15(1) and (3) thereof that (i) the data subject has the right to obtain a first copy, free of charge, of his or her personal data undergoing processing and (ii) the controller is given the option, under certain conditions, to charge a reasonable fee taking administrative costs into account or to refuse to act on a request if it is manifestly unfounded or excessive.  
37      In this instance, it should be noted that a medical practitioner carrying out the processing operations referred to in Article 4(2) of the GDPR concerning his or her patients’ data must be regarded as being a ‘controller’ within the meaning of Article 4(7) of that regulation who is subject to the obligations which that status entails, in particular guaranteeing access to personal data at the request of data subjects.  
38      It must be pointed out that neither the wording of Article 12(5) of the GDPR nor that of Article 15(1) and (3) thereof make the provision, free of charge, of a first copy of personal data conditional upon data subjects putting forward reasons to justify their requests. Therefore, those provisions do not give the controller the possibility of demanding that reasons be given for the request for access submitted by the data subject.  
39      Regarding, secondly, the context in which the provisions referred to above occur, it should be emphasised that Article 12 of the GDPR forms part of Section 1 of Chapter III of that regulation, which concerns, inter alia, the principle of transparency, set out in Article 5(1)(a) thereof.  
40      Article 12 of the GDPR thus sets out the general obligations incumbent on the controller as regards the transparency of information and communications, as well as the rules governing the exercise of the rights of the data subject.  
41      Article 15 of the GDPR, which forms part of Section 2 of Chapter III thereof, concerning information and access to personal data, complements the framework of transparency of that regulation by granting the data subject a right of access to his or her personal data and a right to information regarding the processing of those data.  
42      It should also be noted that, in accordance with recital 59 of the GDPR, ‘modalities should be provided for facilitating the exercise of the data subject’s rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object’.  
43      Given that, as can be seen from paragraph 38 of the present judgment, the data subject is not required to state the reasons for the request for access to data, the first sentence of recital 63 of the GDPR cannot be interpreted as meaning that that request must be rejected if it concerns an objective other than that of becoming aware of the processing of data and verifying the lawfulness of that processing. That recital cannot restrict the scope of Article 15(3) of that regulation as recalled in paragraph 35 of the present judgment.  
44      In that regard, it should be borne in mind that it follows from settled case-law that the preamble to an act of EU law has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner that is clearly contrary to their wording (judgment of 13 September 2018,   
Česká pojišťovna  
, C-287/17, EU:C:2018:707, paragraph 33).  
45      In addition, the second sentence of recital 63 of the GDPR states that the right which data subjects are recognised as having to access personal data includes, as regards data relating to their health, ‘the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided’.  
46      In those circumstances, the right to access data relating to health guaranteed in Article 15(1) of the GDPR cannot be restricted, either by refusing to grant access or by requiring the payment of consideration, to one of the reasons referred to in the first sentence of recital 63 thereof. The same applies as regards the right to obtain a first copy free of charge as provided for in Article 12(5) and Article 15(3) of that regulation.  
47      Thirdly, regarding the objectives pursued by the GDPR, it should be noted that the purpose of that regulation, as indicated by recitals 10 and 11 thereof, is to ensure a consistent and high level of protection of natural persons within the Union, as well as to strengthen and set out in detail the rights of data subjects.  
48      It is precisely in order to achieve that objective that Article 15(1) of the GDPR guarantees the data subject a right to access his or her personal data (see, to that effect, judgment of 22 June 2023,   
Pankki S  
, C-579/21, EU:C:2023:501, paragraph 57 and the case-law cited).  
49      Accordingly, Article 12(5) and Article 15(1) and (3) of the GDPR form part of the provisions intended to guarantee that right of access as well as the transparency, vis-à-vis the data subject, of the manner in which personal data are processed (see, to that effect, judgment of 12 January 2023,   
Österreichische Post (Information regarding the recipients of personal data)  
, C-154/21, EU:C:2023:3, paragraph 42).  
50      The principle that the first copy of the data should be free of charge and the lack of a need to rely on a specific reason to justify the request for access necessarily contribute to facilitating the exercise, by the data subject, of the rights conferred on him or her by the GDPR.  
51      Consequently, given the importance which the GDPR ascribes to the right to access personal data undergoing processing, as guaranteed in Article 15(1) thereof, for achieving such objectives, the exercise of that right cannot be made subject to conditions which have not been expressly laid down by the EU legislature, such as the obligation to rely on one of the reasons referred to in the first sentence of recital 63 of that regulation.  
52      Having regard to all of the foregoing, the answer to the first question is that Article 12(5) and Article 15(1) and (3) of the GDPR must be interpreted as meaning that the controller is under an obligation to provide the data subject, free of charge, with a first copy of his or her personal data undergoing processing, even where the reason for that request is not related to those referred to in the first sentence of recital 63 of that regulation.  
   
The second question  
53      By its second question, the referring court asks, in essence, whether Article 23(1)(i) of the GDPR is to be interpreted as permitting a piece of national legislation, adopted prior to the entry into force of that regulation, which, with a view to protecting the economic interests of the controller, makes the data subject bear the costs of a first copy of his or her personal data undergoing processing.  
54      In the first place, regarding the question whether only national measures adopted after the entry into force of the GDPR are capable of falling within the scope of Article 23(1) thereof, it should be emphasised that the wording of that provision contains no indication in that regard.  
55      Indeed, Article 23(1) of the GDPR merely indicates that a legislative measure of a Member State may restrict the scope of the obligations and rights provided for in Articles 12 to 22 of that regulation in so far as that measure corresponds to the rights and obligations provided for in those articles and when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure to safeguard, inter alia, the protection of the rights and freedoms of others.  
56      Consequently, Article 23(1) of the GDPR does not exclude from its scope national legislative measures adopted prior to the entry into force of that regulation in so far as those measures satisfy the conditions laid down in that provision.  
57      In the second place, regarding the question whether a piece of national legislation which, with a view to protecting the economic interests of persons providing treatment, makes the patient bear the costs connected with the provision of a first copy of the medical records requested by that patient, is covered by Article 23(1)(i) of the GDPR, it should be borne in mind, first, that, as is apparent from paragraphs 31 and 33 to 36 of the present judgment, under Article 12(5) and Article 15(1) and (3) of that regulation, the data subject is recognised as having a right to obtain a first copy, free of charge, of his or her personal data undergoing processing.  
58      However, the second sentence of Article 15(3) of the GDPR authorises the controller to charge a reasonable fee, based on administrative costs, for any further copies. Furthermore, Article 12(5) of that regulation, read in the light of Article 15(1) and (3) thereof, permits the controller to protect itself against abuse of the right of access by charging a reasonable fee in the case of a manifestly unfounded or excessive request.  
59      Secondly, pursuant to recital 4 of that regulation, the right to the protection of personal data is not an absolute right and must be balanced against other fundamental rights, in accordance with the principle of proportionality. Thus, the GDPR respects all the fundamental rights and observes the freedoms and principles recognised by the Charter of Fundamental Rights, as enshrined by the Treaties (judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 53).  
60      In fact, Article 15(4) of the GDPR provides that ‘the right to obtain a copy … shall not adversely affect the rights and freedoms of others’.  
61      Similarly, Article 23(1)(i) of that regulation recalls that a restriction of the scope of the obligations and rights provided for in, inter alia, Article 15 thereof is possible ‘when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard … the protection of … the rights and freedoms of others’.  
62      Consequently, it follows from paragraphs 59 to 61 of the present judgment that the right which the data subject is recognised as having to obtain a first copy, free of charge, of his or her personal data undergoing processing is not absolute.  
63      Thirdly, only considerations relating to, inter alia, the protection of the rights and freedoms of others would be such as to justify a restriction of that right, in so far as such a restriction respects the essence thereof and is a necessary and proportionate measure to safeguard that protection, as provided for in Article 23(1)(i) of the GDPR.  
64      As is apparent from the order for reference, the charging system provided for in the second sentence of subparagraph 2 of Paragraph 630g of the BGB permits the person providing treatment to make the patient bear the costs connected with the provision of a first copy of his or her medical records. The referring court emphasises that that system is intended, primarily, to protect the economic interests of persons providing treatment, which deters patients from making needless requests for copies of their medical records. Thus, in so far as the essential objective of the piece of national legislation at issue in the main proceedings is to protect the economic interests of persons providing treatment, which it is for the referring court to ascertain, such considerations cannot be included in the ‘rights and freedoms of others’ referred to in Article 23(1)(i) of the GDPR.  
65      First, such a piece of legislation deters not only needless requests, but also requests seeking to obtain, for a legitimate reason, a first copy, free of charge, of processed personal data. Consequently, it is necessarily in breach of the principle that the first copy should be free of charge and thereby undermines the effectiveness of the right of access provided for in Article 15(1) of the GDPR, as well as, as a result, the protection guaranteed by that regulation.  
66      Secondly, it is not apparent from the order for reference that the interests protected by that piece of national legislation go beyond considerations of a purely administrative or economic nature.  
67      In that regard, it should be emphasised that the economic interests of controllers were taken into account by the EU legislature under Article 12(5) and the second sentence of Article 15(3) of the GDPR, which, as has been recalled in paragraph 58 of the present judgment, define the circumstances in which the controller may charge a fee connected with the provision of a copy of personal data undergoing processing.  
68      In those circumstances, the pursuit of the objective connected with the protection of the economic interests of persons providing treatment cannot justify a measure leading to the undermining of the right to obtain, free of charge, a first copy and, as a result, of the effectiveness of the data subject’s right of access to his or her personal data undergoing processing.  
69      Having regard to all of the foregoing, the answer to the second question is that Article 23(1)(i) of the GDPR must be interpreted as meaning that a piece of national legislation adopted prior to the entry into force of that regulation is capable of falling within the scope of that provision. However, such a possibility does not permit the adoption of a piece of national legislation which, with a view to protecting the economic interests of the controller, makes the data subject bear the costs of a first copy of his or her personal data undergoing processing.  
   
The third question  
70      By its third question, the referring court asks, in essence, whether the first sentence of Article 15(3) of the GDPR is to be interpreted as meaning that, in the context of a doctor-patient relationship, the right to obtain a copy of personal data undergoing processing means the data subject is to be provided with a full copy of the documents included in his or her medical records and containing his or her personal data, or solely with a copy of those data as such.  
71      First of all, the Court has held that, according to its wording, the first sentence of Article 15(3) of the GDPR confers on the data subject the right to obtain a faithful reproduction of his or her personal data, understood in a broad sense, that are subject to operations that can be classified as ‘processing’ carried out by the controller (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 28).  
72      Next, the first sentence of Article 15(3) of the GDPR cannot be interpreted as establishing a separate right from that provided for in Article 15(1) thereof. Furthermore, the term ‘copy’ does not relate to a document as such, but to the personal data which it contains and which must be complete. The copy must therefore contain all the personal data undergoing processing (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 32).  
73      Lastly, regarding the objectives pursued by Article 15 of the GDPR, the purpose of that regulation is to strengthen and set out in detail the rights of data subjects. Thus, the right of access provided for in that provision must enable the data subject to ensure that the personal data relating to him or her are correct and that they are processed in a lawful manner. Furthermore, the copy of the personal data undergoing processing, which the controller must provide pursuant to the first sentence of Article 15(3) of the GDPR, must have all the characteristics necessary for the data subject effectively to exercise his or her rights under that regulation and must, consequently, reproduce those data fully and faithfully (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraphs 33, 34 and 39).  
74      In particular, in order to ensure that the information provided by the controller is easy to understand, as is required by Article 12(1) of the GDPR, read in the light of recital 58 of that regulation, the reproduction of extracts from documents or even of entire documents which contain, inter alia, the personal data undergoing processing may prove to be essential where the contextualisation of the data processed is necessary in order to ensure the data are intelligible (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 41).  
75      Consequently, the right to obtain from the controller a copy of the personal data undergoing processing means that the data subject must be given a faithful and intelligible reproduction of all those data. That right entails the right to obtain copies of extracts from documents or even of entire documents which contain, inter alia, those data, if the provision of such a copy is essential in order to enable the data subject to exercise effectively the rights conferred on him or her by that regulation (judgment of 4 May 2023,   
Österreichische Datenschutzbehörde and CRIF  
, C-487/21, EU:C:2023:369, paragraph 45).  
76      Regarding the information at issue in the case in the main proceedings, it should be noted that the GDPR identifies the material of which the applicant at first instance in the main proceedings should be able to request a copy. Thus, as regards personal data relating to health, recital 63 of that regulation specifies that the right of access of data subjects includes ‘the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided’.  
77      In that regard, as was noted, in essence, by the Advocate General in points 78 to 80 of his Opinion, it is because of the sensitive nature of personal data relating to the health of natural persons that the EU legislature thus highlighted the importance of ensuring that those persons are given access to the data contained in their medical records as fully and precisely as possible, but also in a form which is intelligible.  
78      Regarding examination results, assessments by treating physicians and treatments or interventions provided to a patient, which, as a general rule, involve a large amount of technical data, or even images, the provision of a simple summary or a compilation of those data by the medical practitioner, in order to present them in an aggregated form, could create the risk of some relevant data being omitted or incorrectly reproduced, or, in any event, of it being made harder for the patient to verify how accurate and exhaustive those data are and to understand those data.  
79      Having regard to all of the foregoing, the answer to the third question is that the first sentence of Article 15(3) of the GDPR must be interpreted as meaning that, in the context of a doctor-patient relationship, the right to obtain a copy of personal data undergoing processing means that the data subject must be given a faithful and intelligible reproduction of all those data. That right entails the right to obtain a full copy of the documents included in his or her medical records and containing, inter alia, those data if the provision of such a copy is essential in order to enable the data subject to verify how accurate and exhaustive those data are, as well as to ensure they are intelligible. Regarding data relating to the health of the data subject, that right includes in any event the right to obtain a copy of the data in his or her medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided to him or her.  
   
Costs  
80      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
1.        
Article 12(5) and Article 15(1) and (3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),  
must be interpreted as meaning that the controller is under an obligation to provide the data subject, free of charge, with a first copy of his or her personal data undergoing processing, even where the reason for that request is not related to those referred to in the first sentence of recital 63 of that regulation.  
2.        
Article 23(1)(i) of Regulation 2016/679  
must be interpreted as meaning that a piece of national legislation adopted prior to the entry into force of that regulation is capable of falling within the scope of that provision. However, such a possibility does not permit the adoption of a piece of national legislation which, with a view to protecting the economic interests of the controller, makes the data subject bear the costs of a first copy of his or her personal data undergoing processing.  
3.        
The first sentence of Article 15(3) of Regulation 2016/679  
must be interpreted as meaning that, in the context of a doctor-patient relationship, the right to obtain a copy of personal data undergoing processing means that the data subject must be given a faithful and intelligible reproduction of all those data. That right entails the right to obtain a full copy of the documents included in his or her medical records and containing, inter alia, those data if the provision of such a copy is essential in order to enable the data subject to verify how accurate and exhaustive those data are, as well as to ensure they are intelligible. Regarding data relating to the health of the data subject, that right includes in any event the right to obtain a copy of the data in his or her medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided to him or her.

ID: e4af5ce7-2fd2-4954-ab5b-7c199ccf92f7

of 9 Jul 2020, C-272/19 (  
Land Hessen  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Restrictions   
General data protection law   
 >   
Chapter III - Rights of the data subject   
 >   
Right of access   
   
JUDGMENT OF THE COURT (Third Chamber)  
9 July 2020 (\*)  
(Reference for a preliminary ruling — Article 267 TFEU — Concept of ‘court or tribunal’ — Protection of natural persons with regard to the processing of personal data — Regulation (EU) 2016/679 — Scope — Article 2(2)(a) — Meaning of ‘activity which falls outside the scope of Union law’ — Article 4(7) — Concept of ‘controller’ — Petitions Committee of the parliament of a Federated State of a Member State — Article 15 — Right of access by the data subject)  
In Case C-272/19,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden, Germany), made by decision of 27 March 2019, received at the Court on 1 April 2019, in the proceedings  
VQ  
v  
Land  
 Hessen,  
THE COURT (Third Chamber),  
composed of A. Prechal, President of the Chamber, L.S. Rossi (Rapporteur), J. Malenovský, F. Biltgen and N. Wahl, Judges,  
Advocate General: M. Szpunar,  
Registrar: A. Calot Escobar,  
having regard to the written procedure,  
after considering the observations submitted on behalf of:  
–        VQ, by A.-K. Pantaleon, genannt Stemberg, Rechtsanwältin,  
–          
Land  
 Hessen, by H.-G. Kamann, M. Braun and L. Hesse, Rechtsanwälte,  
–        the German Government, by J. Möller, M. Hellmann and A. Berg, acting as Agents,  
–        the Czech Government, by M. Smolek, O. Serdula and J. Vláčil, acting as Agents,  
–        the Estonian Government, by N. Grünberg, acting as Agent,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the European Commission, by H. Krämer, D. Nardi and F. Erlbacher, acting as Agents,  
having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of (i) Article 4(7) and Article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1), and (ii) Article 267 TFEU, read together with the second paragraph of Article 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in proceedings between VQ and   
Land  
 Hessen (Germany) concerning the lawfulness of the rejection by the President of the Hessischer Landtag (the Parliament of   
Land   
 Hessen) of VQ’s application for access to the personal data concerning him, as recorded by the Petitions Committee of that parliament.  
   
Legal context  
   
European Union law  
   
Directive 95/46/EC  
3        Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), which was repealed by Regulation 2016/679, contained an Article 3, headed ‘Scope’, which provided:  
‘1.      This Directive shall apply to the processing of personal data wholly or partly by automated means, and to the processing otherwise than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Directive shall not apply to the processing of personal data:  
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
–        by a natural person in the course of a purely personal or household activity.’  
   
Regulation 2016/679  
4        Recitals 16 and 20 of Regulation 2016/679 state:  
‘(16)      This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.  
…  
(20)      While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.’  
5        Article 2 of that regulation, headed ‘Material scope’, provides:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the [Treaty on European Union];  
(c)      by a natural person in the course of a purely personal or household activity;  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.  
…’  
6        Article 4 of that regulation, headed ‘Definitions’, provides:  
‘For the purposes of this Regulation:  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its appointment may be provided for by Union or Member State law;  
…’  
7        Article 15(1) of that regulation, that article being headed ‘Right of access by the data subject’, provides:  
‘The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:  
…’  
8        Article 23(1) of Regulation 2016/679, that article being headed ‘Restrictions’, provides:  
‘Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:  
(a)      national security;  
(b)      defence;  
(c)      public security;  
(d)      the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;  
(e)      other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;  
(f)      the protection of judicial independence and judicial proceedings;  
(g)      the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;  
(h)      a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a) to (e) and (g);  
(i)      the protection of the data subject or the rights and freedoms of others;  
(j)      the enforcement of civil law claims.’  
   
German law  
   
Federal law  
9        Article 97 of the Grundgesetz für die Bundesrepublik Deutschland (Basic Law for the Federal Republic of Germany) provides:  
‘(1)      Judges shall be independent and subject only to the law.  
(2)      Judges duly appointed for life to full-time judicial office may be involuntarily dismissed, permanently or temporarily suspended, transferred or retired from that office before the expiry of their term of office only by virtue of a judicial decision and on the grounds and in the manner specified by the law. The legislature may set age limits for the retirement of judges appointed for life. In the event of changes in the structure of the courts or in their areas of jurisdiction, judges may be transferred to another court or removed from office, provided that they retain their full salary.’  
10      Paragraph 26 of the Deutsches Richtergesetz (the German Judiciary Act; ‘the DRiG’) is worded as follows:  
‘(1)      A judge shall be subject to supervision only to the extent that his or her independence is not adversely affected.  
(2)      Without prejudice to subparagraph (1), supervision shall also include the power to censure a judge for the improper performance of his or her duties and to warn him or her to perform his or her duties promptly and properly.  
(3)      Where a judge maintains that a supervisory measure adversely affects his or her independence, a court shall, at the request of that judge, give a ruling in compliance with this Act.’  
   
The law of   
Land  
 Hessen  
11      Article 126 of the Verfassung des Landes Hessen (Constitution of   
Land   
 Hessen) provides:  
‘(1)      Judicial authority shall be exercised exclusively by the lawfully established courts and tribunals.  
(2)      Judges shall be independent and subject only to the law.’  
12      Article 127 of that Constitution is worded as follows:  
‘(1)      Judges duly appointed to full-time judicial office shall be appointed for life.  
(2)      Judges shall be appointed for life only if, after temporary engagement for a probation period the duration of which is to be determined by statute, their character and judicial activity is demonstrably such as to ensure that they will perform their duties in the spirit of democracy and with understanding of society.  
(3)      A decision on temporary engagement and appointment for life shall be made jointly by the Minister of Justice and a judicial appointments committee.  
…’  
13      Paragraph 2b of the Hessisches Richtergesetz (the   
Land   
 Hessen Judiciary Act; ‘the HRiG’) states:  
‘The assessment of the ability, competences and professional performance of the judges shall be regulated by the Guidelines of the Minister of Justice.’  
14      Paragraph 3 of the HRiG provides:  
‘Judges shall be appointed by the Minister of Justice.’  
15      Paragraph 18 of the Verwaltungsgerichtsordnung (Code of Administrative Procedure), is worded as follows:  
‘For the purpose of covering staff requirements of a temporary nature, an established public servant having the requisite qualifications for judicial office may be appointed as an acting judge for a period of at least two years, but for no longer than the duration of his or her main office. Paragraph 15(1), first and third sentences, and (2) of the [DRiG] shall apply   
mutatis mutandis  
.’  
16      Paragraph 30(1) of the Hessisches Datenschutz- und Informationsfreiheitsgesetz (Law of   
Land   
 Hessen on the protection of data and freedom of information), which adapts the law of   
Land   
 Hessen in the area of data protection to, inter alia, Regulation 2016/679, provides:  
‘With the exception of Paragraphs 15 and 29, the provisions of this law shall apply to the [Parliament of   
Land  
 Hessen] solely to the extent that [that parliament] plays a part in administrative matters, including the economic matters of [that parliament], staff management or the implementation of legislative provisions compliance with which is the responsibility of the President of [that parliament]. Further, [that parliament] shall adopt an internal regulation concerning data protection compatible with its constitutional status. …’  
17      Annex 2 to the Geschäftsordnung des Hessischen Landtags (Internal regulation of the Parliament of   
Land   
 Hessen) of 16 December 1993 contains the guidelines relating to the treatment of information that is classified in the hands of the Parliament of   
Land  
 Hessen of 1986, which state, in Paragraph 13 thereof, headed ‘Protection of private confidential information’:  
‘(1)      In so far as the protection of personal, professional or business confidential information requires it, the files, other documents and deliberations of the committees must be kept secret. That applies in particular with respect to files relating to tax matters and petitions. …  
(2)      The right to consult such files or documents shall be reserved to the members of the competent committee. The same applies to consultation of the minutes of deliberations of the committees on issues requiring confidentiality, within the meaning of subparagraph 1. The committee shall decide on the distribution of the minutes.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
18      After his submission of a petition to the Petitions Committee of the Parliament of   
Land  
 Hessen, VQ applied to that committee, on the basis of Article 15 of Regulation 2016/679, for access to the personal data concerning him, recorded by that committee when dealing with his petition.  
19      The President of the Parliament of   
Land  
 Hessen decided to reject that application, on the ground that the petition procedure constitutes a function of the parliament and that the parliament was outside the scope of Regulation 2016/679.  
20      On 22 March 2013, VQ brought an action before the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden, Germany) challenging the decision of the President of the Parliament of   
Land  
 Hessen rejecting his application.  
21      That court notes that, taking into consideration, inter alia, Paragraph 13 of the guidelines relating to the treatment of information that is classified in the hands of the Parliament of   
Land  
 Hessen of 1986, German law grants no right of access to personal data in the context of a petition such as that in the main proceedings.  
22      However, that court is uncertain, first, whether the Petitions Committee of the Parliament of   
Land  
 Hessen can be categorised as a ‘public authority’, within the meaning of Article 4(7) of Regulation 2016/679, and may, in this instance, be considered to be the ‘controller’ of VQ’s personal data. If so, VQ could claim a right of access under Article 15 of that regulation.  
23      Regulation 2016/679 does not, however, provide any definition of the concept of ‘public authority’. In the view of the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden), that expression can be understood in a functional sense or in an institutional sense. Taking the first sense, ‘public authorities’ comprise all public bodies that carry out public administrative tasks, including, consequently, the Parliament of   
Land  
 Hessen when it carries out such tasks. Taking the second sense, the Petitions Committee of that parliament is an independent body, and therefore a public authority, in the institutional sense. It does not take part in the legislative activity of that parliament given that, first, its activity has no binding effect and, second, it has no right to initiate legislation and no right to enact regulations, its actions always being dependent on a citizen’s petition being submitted and the content of the petition.  
24      Further, since Article 2(2) of Regulation 2016/679 does not exclude bodies or institutions acting in a judicial or legislative capacity, that provision implies that the concept of public services and therefore the concept of a public authority should be construed broadly. Accordingly, from the perspective of the right to submit a petition, there is nothing to distinguish that committee from any other administrative authority of   
Land  
 Hessen.  
25      The Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) considers, consequently, that the Petitions Committee of the Parliament of   
Land  
 Hessen is a ‘public authority’, within the meaning of Article 4(7) of that regulation and that there is no reason, in this case, to exclude a right of access under Article 15 of that regulation.  
26      However, that court is uncertain, in the second place, whether it itself can be considered to be a ‘court or tribunal’, within the meaning of Article 267 TFEU, read together with the second paragraph of Article 47 of the Charter, in the light of the criteria set out by the Court in that regard, in particular the criterion pertaining to the independence of the body concerned.  
27      In that regard, the referring body states that that the requirement of independence has two aspects. The first aspect, which is external, assumes that the body concerned exercises its functions wholly autonomously, without being subordinated to any other body and without taking orders or instructions from any source whatsoever, and is thus protected against external interventions or pressure liable to jeopardise the independent judgment of its members as regards proceedings before them. The second aspect, which is internal in nature, is linked to the concept of impartiality and seeks to ensure that an equal distance is maintained from the parties to the proceedings and their respective interests with regard to the subject matter of those proceedings. That aspect requires objectivity and the absence of any interest in the outcome of the proceedings apart from the strict application of the rule of law.  
28      As regards the external aspect of independence, the connection of a court or tribunal to the Ministry of Justice means that that court or tribunal cannot function wholly autonomously. In this case, the organisation of the courts or tribunals in   
Land  
 Hessen is determined by the Ministry of Justice of that   
Land  
. In particular, that ministry determines the means of communication (telephone, fax, Internet and so forth) and the IT facilities, notably the ‘HessenPC’, designed for the public services, with a central service provider, the Hessische Zentrale für Datenverarbeitung (  
Land  
 Hessen Centre for the data processing), which is part of the Ministry for Finance of   
Land  
 Hessen. The latter ensures also the maintenance of all those facilities, so that the administrative authority has the possibility of obtaining access to all the data of the courts or tribunals.  
29      The mere risk of political influence being applied to the courts or tribunals, by means of, inter alia, the facilities or staff allocated by the Ministry of Justice, is sufficient to create a risk of interference in their decisions and to affect the independence of the court or tribunals in the performance of their tasks. It would be sufficient for that purpose if there was an imagined pressure to achieve rapid settlement of cases using a workload statistic managed by that ministry.  
30      Further, the courts or tribunals of   
Land  
 Hessen have no independent control in the area of data protection, since the bulk of the processing of data is prescribed, in essence, by the Ministry of Justice of   
Land  
 Hessen, with no supervision by the courts as mentioned in recital 20 of Regulation 2016/679.  
31      As regards the internal aspect of independence, the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) states that German constitutional law does not guarantee the institutional independence of the courts or tribunals.  
32      First, as is clear from Paragraphs 2b and 3 of the HRiG, the appointment, appraisal and promotion of judges, including those who are members of the referring court, are matters for the Minister of Justice of   
Land  
 Hessen. It follows that the provisions of public service law are applicable to them, so that, inter alia, decisions on work-related travel abroad of judges, such as that undertaken as part of the European Judicial Training Network, have to be made by that minister.  
33      Next, in accordance with Paragraph 18 of the code of administrative procedure, in order to meet a temporary need for staff, a public official can be appointed as a temporary judge. Such a judge could come from a public authority which is the defendant in judicial proceedings brought before him or her.  
34      Moreover, the Ministry of Justice of   
Land  
 Hessen records the professional contact details of all the judges in a human resources information management system which is the responsibility of the government of   
Land   
 Hessen, so that all the administrative authorities of that   
Land   
 can obtain access to that data, even when they may be a party in a case brought before those judges.  
35      Last, the Ministry of Justice also decides on the number of judges and number of posts at each court or tribunal, on the ‘non-judicial’ staff assigned, in fact, to the executive, and on the extent of the IT facilities of each court or tribunal.  
36      Accordingly, the court or tribunals have merely a functional independence in so far as the judges alone are independent and subject to the law, in accordance with Paragraph 126 of the Constitution of   
Land  
 Hessen. However, by itself, that functional independence is insufficient to protect the court or tribunals from any external influence.  
37      The conclusion of the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) is that, probably, it does not satisfy the conditions laid down in the second paragraph of Article 47 of the Charter governing whether it can be regarded as an independent and impartial tribunal.  
38      In those circumstances, the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘(1)      Is [Regulation 2016/679], in particular [its] Article 15, [headed “Right of access by the data subject”], applicable to the committee of a parliament of a Federated State of a Member State that is responsible for dealing with the petitions of citizens — in this case the Petitions Committee of the Parliament of   
Land  
 Hessen — and is that committee to be regarded in that connection as a public authority within the meaning of Article 4(7) of Regulation 2016/679?  
(2)      Is the referring court an independent and impartial court or tribunal within the meaning of Article 267 TFEU read in conjunction with the second paragraph of Article 47 of [the Charter]?’  
   
The jurisdiction of the Court  
39      In its observations, the Polish Government calls into question the jurisdiction of the Court, in particular its jurisdiction to give a ruling on the second question, given that EU law does not regulate the judicial organisation of the Member States and that, consequently, that question falls solely within the scope of national law.  
40      Suffice it to state, in that regard, that the request for a preliminary ruling concerns the interpretation of EU law, whether of Regulation 2016/679 or of Article 267 TFEU, read together with Article 47 of the Charter.  
41      In those circumstances, the Court plainly has jurisdiction to give a ruling on that request in its entirety, that is, on both the first and the second question (see, to that effect, judgment of 19 November 2019,   
A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)  
, C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraphs 74 and 75).  
   
The admissibility of the request for a preliminary ruling  
42      By its second question, the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) expresses doubt as to its own status as a ‘court or tribunal’, within the meaning of Article 267 TFEU, read in the light of Article 47 of the Charter. Accordingly, it is in fact inviting the Court to examine the admissibility of its request for a preliminary ruling, given that being a ‘court or tribunal’, within the meaning of Article 267, is a condition of that admissibility and, consequently, a prerequisite of the interpretation by the Court of the provision of EU law specified in the first question.  
43      In accordance with settled case-law, in order to determine whether a body making a reference is a ‘court or tribunal’, within the meaning of Article 267 TFEU, which is a question governed by EU law alone, and therefore to determine whether the request for a preliminary ruling is admissible, the Court takes account of a number of factors, such as whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is   
inter partes  
, whether it applies rules of law and whether it is independent (see, to that effect, judgment of 21 January 2020,   
Banco de Santander  
,   
 C-274/14, EU:C:2020:17, paragraph 51 and the case-law cited).  
44      The doubts expressed by the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) concern its own independence from the legislature or from the executive. Those doubts are based on the following circumstances: (i) the judges are appointed and promoted by the Minister of Justice; (ii) the appraisal of judges is undertaken by the Ministry of Justice according to the same rules as are applicable to public officials; (iii) the personal data and professional contact details of the judges are managed by that ministry, which thus has access to that data; (iv) to cover temporary staff requirements, public officials can be appointed as temporary judges; and (v) the Minister of Justice prescribes the external and internal organisation of the courts or tribunals, determines the allocation of staff, means of communication and IT facilities of the courts or tribunals and also decides on the work-related travel abroad undertaken by the judges.  
45      In that regard, it must be recalled that the independence of the judges of the Member States is of fundamental importance for the EU legal order in various respects. It is informed, first, by the principle of the rule of law, which is one of the values on which, under Article 2 TEU, the Union is founded and which are common to the Member States, and by Article 19 TEU, which gives concrete expression to that value and entrusts shared responsibility for ensuring judicial review within the EU legal order to national courts or tribunals (see, to that effect, judgment of 27 February 2018,   
Associação Sindical dos Juízes Portugueses  
, C-64/16, EU:C:2018:117, paragraph 32). Second, that independence is a necessary condition if individuals are to be guaranteed, within the scope of EU law, the fundamental right to an independent and impartial tribunal laid down in Article 47 of the Charter, which is of cardinal importance as a guarantee of the protection of all the rights that individuals derive from EU law (see, to that effect, inter alia, judgment of 26 March 2020,   
Review Simpson  
 v   
Council  
 and  
 HG   
v   
 Commission  
, C-542/18 RX-II and C-543/18 RX II, EU:C:2020:232, paragraphs 70 and 71 and the case-law cited). Last, that independence is essential to the proper working of the judicial cooperation system embodied by the preliminary ruling mechanism under Article 267 TFEU, in that that mechanism may be activated only by a body responsible for applying EU law, which satisfies, inter alia, that criterion of independence (see, in particular, judgment of 21 January 2020,   
Banco de Santander  
,   
 C-274/14, EU:C:2020:17, paragraph 56 and the case-law cited).  
46      Accordingly, in order to determine the admissibility of a request for a preliminary ruling, the criterion relating to independence which the referring body must satisfy before it can be considered to be a ‘court or tribunal’, within the meaning of Article 267 TFEU, may be assessed solely in the light of that provision.  
47      It follows, as stated by the European Commission, that, in this instance, that assessment must relate to the independence of the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) solely in the context of the dispute in the main proceedings, which relates, as is stated in paragraphs 22 to 25 of the present judgment, to the interpretation of EU law, namely Regulation 2016/679.  
48      In that regard, some factors to which the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) draws attention are plainly of no relevance for that assessment.  
49      That must be said, in the first place, of the rules relating to the procedures for the appointment of temporary judges, since such judges are not members of the formation of the court, in this instance, which consists solely of the President of the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden).  
50      As regards, in the second place, the role of the Ministry of Justice of   
Land  
 Hessen with respect to the management of work-related travel of judges or the organisation of the court or tribunals, the determination of staff numbers, the management of means of communication and IT facilities, as well as the management of personal data, suffice it to state that the request for a preliminary ruling contains no information from which it can be ascertained to what extent those factors are liable to call into question, in the main proceedings, the independence of the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden).  
51      It remains, therefore, in essence, necessary to determine the alleged influence that the legislature or the executive are capable of exercising over judges who are members of that administrative court by reason of their involvement in the appointment, promotion and appraisal of those judges.  
52      In accordance with settled case-law, the guarantees of the independence and impartiality of the courts and tribunals of the Member States require rules, particularly as regards the composition of the body and the appointment and length of service of its members, and as regards grounds for withdrawal by, challenges to, and dismissal of its members, in order to dispel any reasonable doubt in the minds of litigants as to the imperviousness of that body to external factors and its neutrality with respect to the interests before it (judgment of 21 January 2020,   
Banco de Santander  
,   
 C-274/14, EU:C:2020:17, paragraph 63 and the case-law cited).  
53      In that regard, the German Government states that, in this instance, the judiciary has an autonomous status within the public service, which is ensured, inter alia, by the guarantee of irremovability laid down in Paragraph 97 of the Basic Law for the Federal Republic of Germany, by the fact that there exist civil service courts with jurisdiction over judges for the judicial protection of judges, and by the appointment procedure, in which the Judicial Appointments Committee plays a crucial role. That committee, provided for in Article 127 of the Constitution of   
Land  
 Hessen, is composed of seven members designated by the parliament of that   
Land  
, five members of the judiciary and, by annual rotation, the President of one of the two Bar Associations of   
Land  
 Hessen. The members designated by the parliament, in proportion to the composition of that institution, serve to ensure the democratic legitimacy of that committee.  
54      As regards the conditions governing the appointment of the judge sitting in the referring court, it must be recalled at the outset that the mere fact that the legislative authorities play a part in the process for appointing a judge does not give rise to a relationship of subordination to those authorities or to doubts as to the judge’s impartiality, if, once appointed, he or she is not subject to any pressure and does not receive any instruction in performing the duties of his or her office (see, to that effect, judgment of 19 November 2019,   
A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)  
, C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraph 133 and the case-law cited).  
55      The Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) appears, however, also to have doubts as to the compatibility of the composition of the Judicial Appointments Committee with the principle of independence, given that the majority of its members are chosen by the legislature.  
56      However, that fact cannot, in itself, give rise to any doubt as to the independence of the referring court. The assessment of the independence of a national court or tribunal must, including from the perspective of the conditions governing the appointment of its members, be made in the light of all the relevant factors.  
57      It must be recalled, in that regard, that, where a national court or tribunal has submitted to the Court a number of factors which, in its view, call into question the independence of a committee involved in the appointment of judges, the Court has held that, although one or other of the factors indicated by that court or tribunal may be such as to escape criticism per se and may fall, in that case, within the competence of, and choices made by, the Member States, those factors, when taken together, in addition to the circumstances in which those choices were made, may, by contrast, throw doubt on the independence of a body involved in the procedure for the appointment of judges, despite the fact that, when those factors are taken individually, that conclusion is not inevitable (judgment of 19 November 2019,   
A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)  
, C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraph 142).  
58      In this instance, it cannot be concluded that a committee such as that at issue in the main proceedings is not independent solely because of the factor mentioned in paragraph 55 of the present judgment.  
59      As regards the conditions governing the appraisal and promotion of judges, which are also called into question by the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden), suffice it to state that the documents submitted to the Court contain no indication as to how the manner in which the executive uses its powers in that regard are such as to engender legitimate doubts, particularly in the minds of litigants, concerning whether the judge concerned is impervious to external elements and whether he or she is impartial with respect to the opposing interests that may be brought before him or her.  
60      In the light of the foregoing, the factors to which the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) draws attention in support of the doubts that it expresses in relation to its own independence cannot, in themselves, be sufficient ground for a conclusion that those doubts are well-founded and that that court is not independent, notwithstanding all the other rules laid down by the legal order of which that administrative tribunal forms part and designed to ensure its independence, rules which include, in particular, those mentioned in paragraph 53 of the present judgment.  
61      In those circumstances, the Verwaltungsgericht Wiesbaden (Administrative Court of Wiesbaden) must, in this instance, be considered to be a ‘court or tribunal’, within the meaning of Article 267 TFEU. The request for a preliminary ruling is therefore admissible.  
62      It must be made clear that that conclusion has no effect on the examination of the admissibility of the second question referred for a preliminary ruling, which, as such, is inadmissible. Since that question concerns the interpretation of Article 267 TFEU itself, which is not at issue for the purposes of resolving the dispute in the main proceedings, the interpretation requested by that question is not objectively required for the decision which must be made by the referring court (see, to that effect, order of 25 May 1998,   
Nour  
, C-361/97, EU:C:1998:250, paragraph 15 and the case-law cited).  
   
The request for a preliminary ruling  
63      By its request for a preliminary ruling, the referring court asks the Court, in essence, whether Article 4(7) of Regulation 2016/679 must be interpreted as meaning that the Petitions Committee of the parliament of a Federated State of a Member State must be categorised as a ‘controller’, within the meaning of that provision, so that the processing of personal data carried out by that committee falls within the scope of that regulation, and, in particular, of Article 15 thereof.  
64      In order to answer that question, it must, first, be noted that Article 4(7) of that regulation defines the ‘controller’ as being the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.  
65      Accordingly, the definition of the concept of ‘controller’ in Regulation 2016/679 is not confined to public authorities, but, as emphasised by the Czech Government, is sufficiently wide to include any body which, alone or jointly with others, determines the purposes and means of the processing of personal data.  
66      As regards, second, the observations of   
Land  
 Hessen to the effect that the activities of a parliamentary committee fall outside the scope of EU law, within the meaning of Article 2(2) of Regulation 2016/679, it must be recalled that the Court has already had occasion to state, in relation to Article 3(2) of Directive 95/46, which is based on Article 100a of the EC Treaty (which became, after amendment, Article 95 EC), that recourse to that legal basis does not presuppose the existence of an actual link with free movement between Member States in every situation referred to by the measure founded on that legal base and that it is not appropriate to interpret the expression ‘activity which falls outside the scope of [Union] law’ as having a meaning which would require it to be determined in each individual case whether the specific activity at issue directly affected freedom of movement between Member States (judgment of 6 November 2003,   
Lindqvist  
,   
C-101/01, EU:C:2003:596, paragraphs 40 and 42).  
67      That applies a fortiori with respect to Regulation 2016/679, which is based on Article 16 TFEU, which states that the European Parliament and the Council of the European Union are to lay down the rules relating to the protection of individuals with regard to the processing of personal data by, in particular, Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data; Article 2(2) of that regulation corresponds, in essence, to Article 3(2) of Directive 95/46.  
68      Third, since Article 2(2)(a) of that regulation constitutes an exception to the very wide definition of the scope of that regulation set out in Article 2(1) of that regulation, Article 2(2)(a) must be interpreted restrictively.  
69      Admittedly, the Court has, in essence, stated that the activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 (in other words, the activities provided for by Titles V and VI of the Treaty on European Union and data processing operations concerning public security, defence, State security and activities in areas of criminal law) are, in all circumstances, activities of the States or of State authorities, and those activities are intended to define the extent of the exception provided for therein, with the result that that exception applies only to the activities which are expressly listed there or which can be classified in the same category (  
ejusdem generis  
) (judgment of 6 November 2003,   
Lindqvist  
,   
C-101/01, EU:C:2003:596, paragraphs 43 and 44).  
70      However, that fact that an activity is an activity characteristic of the State or of a public authority is not sufficient ground for that exception to be automatically applicable to such an activity. It is necessary that that activity is one of the activities that are explicitly mentioned by that provision or that it can be classified in the same category as those activities.  
71      While the activities of the Petitions Committee of the Parliament of   
Land  
 Hessen are incontestably public and are activities of that   
Land  
, that committee contributing indirectly to the parliamentary activity, the fact remains that not only are those activities political as much as administrative, but it is also not clear from the documents available to the Court that those activities correspond, in this instance, to the activities mentioned in Article 2(2)(b) and (d) of Regulation 2016/679 or that they can be classified in the same category as those activities.  
72      Fourth and last, no exception is provided for in Regulation 2016/679, including in recital 20 and in Article 23 of that regulation, with respect to parliamentary activities.  
73      Consequently, in so far as the Petitions Committee of the Parliament of   
Land  
 Hessen determines, alone or with others, the purposes and means of the processing of personal data, that committee must be categorised as a ‘controller’, within the meaning of Article 4(7) of Regulation 2016/679 and consequently, Article 15 of that regulation is, in this instance, applicable.  
74      It follows from all the foregoing that Article 4(7) of Regulation 2016/679 must be interpreted as meaning that, in so far as a Petitions Committee of the parliament of a Federated State of a Member State determines, alone or with others, the purposes and means of the processing of personal data, that committee must be categorised as a ‘controller’, within the meaning of that provision, and consequently the processing of personal data carried out by that committee falls within the scope of that regulation and, in particular, of Article 15 thereof.  
   
Costs  
75      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
Article 4(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as meaning that, in so far as a Petitions Committee of the parliament of a Federated State of a Member State determines, alone or with others, the purposes and means of the processing of personal data, that committee must be categorised as a ‘controller’, within the meaning of that provision, and consequently the processing of personal data carried out by that committee falls within the scope of that regulation and, in particular, of Article 15 thereof.

ID: ef2cac0d-0e3a-47e8-a273-6b6736ce49d4

Judgment of 19 Oct 2016, C-582/14 (  
Breyer  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Personal Data   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Legitimate interest   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Material Scope - Criminal offence and public security exemption   
   
JUDGMENT OF THE COURT (Second Chamber)  
19 October 2016 (\*)  
(Reference for a preliminary ruling — Processing of personal data — Directive 95/46/EC — Article 2(a) — Article 7(f) — Definition of ‘personal data’ — Internet protocol addresses — Storage of data by an online media services provider — National legislation not permitting the legitimate interest pursued by the controller to be taken into account)  
In Case C-582/14,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 28 October 2014, received at the Court on 17 December 2014, in the proceedings  
Patrick Breyer  
v  
Bundesrepublik Deutschland,  
THE COURT (Second Chamber),  
composed of M. Ilešič, President of the Chamber, A. Prechal, A. Rosas (Rapporteur), C. Toader and E. Jarašiūnas, Judges,  
Advocate General: M. Campos Sánchez-Bordona,  
Registrar: V. Giacobbo-Peyronnel, Administrator,  
having regard to the written procedure and further to the hearing on 25 February 2016,  
after considering the observations submitted on behalf of:  
–        Mr Breyer, by M. Starostik, Rechtsanwalt,  
–        the German Government, by A. Lippstreu and T. Henze, acting as Agents,  
–        the Austrian Government, by G. Eberhard, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,  
–        the European Commission, by P.J.O. Van Nuffel and H. Krämer, and P. Costa de Oliveira and J. Vondung, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 12 May 2016,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 2(a) and 7(f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).  
2        The request has been made in proceedings between Mr Patrick Breyer and the Bundesrepublik Deutschland (Federal Republic of Germany) concerning the registration and storage by the latter of the internet protocol address (‘IP address’) allocated to Mr Breyer when he accessed several internet sites run by German Federal institutions.  
   
Legal context  
   
EU law  
3        Recital 26 of Directive 95/46 reads as follows:   
‘Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.’   
4        Article 1 of that directive provides:   
‘1.      In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.   
2.      Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.’   
5        Article 2 of the same directive provides:   
‘For the purpose of this Directive:  
(a)      “Personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;   
(b)      “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;   
…  
(d)      “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;  
…  
(f)      “third party” shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;  
…’  
6        Article 3 of Directive 95/46, entitled ‘Scope’, provides:   
‘1.      This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.   
2.      This Directive shall not apply to the processing of personal data:   
–        in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,  
…’  
7        Article 5 of that directive reads as follows:   
‘Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.’   
8        Article 7 of the directive is worded as follows:  
‘Member States shall provide that personal data may be processed only if:   
(a)      the data subject has unambiguously given his consent; or   
(b)      processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or   
(c)      processing is necessary for compliance with a legal obligation to which the controller is subject; or   
(d)      processing is necessary in order to protect the vital interests of the data subject; or   
(e)      processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or   
(f)      processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’  
9        Article 13(1) of Directive 95/46 provides:   
‘Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:   
…  
(d)      the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;   
…’  
   
German law  
10      Paragraph 12 of the Telemediengesetz (Law on telemedia) of 26 February 2007 (BGBl. 2007 I, p. 179, ‘TMG’), provides:  
‘(1)      A service provider may collect and use personal data to make telemedia available only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.   
(2)      Where personal data have been supplied in order for telemedia to be made available, a service provider may use them for other purposes only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.   
(3)      Except as otherwise provided, the provisions concerning the protection of personal data which are applicable in the case in question shall apply even if the data are not processed automatically.’   
11      Paragraph 15 of the TMG provides:   
‘(1)      A service provider may collect and use the personal data of a user only to the extent necessary in order to facilitate, and charge for, the use of telemedia (data concerning use). Data concerning use include, in particular:   
1.      particulars for the identification of the user,   
2.      information about the beginning, end and extent of the particular use, and   
3.      information about the telemedia used by the user.   
(2)      A service provider may combine the data concerning use of a user relating to the use of different telemedia to the extent that this is necessary for purposes of charging the user.  
…  
(4)      A service provider may use data concerning use after the end of the use to the extent that they are required for purposes of charging the user (invoicing data). The service provider may block the data in order to comply with existing limits on storage periods laid down by law, statutes or contract.’   
12      Under Paragraph 3(1) of the Bundesdatenschutzgesetz (Federal Data Protection Law) of 20 December 1990 (BGBl. 1990 I, p. 2954, ‘personal data are individual indications concerning the personal or factual circumstances of an identified or identifiable natural person (data subject). …’.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
13      Mr Breyer has accessed several websites operated by German Federal institutions. On the websites, which are accessible to the public, those institutions provide topical information.  
14      With the aim of preventing attacks and making it possible to prosecute ‘pirates’, most of those websites store information on all access operations in logfiles. The information retained in the logfiles after those sites have been accessed include the name of the web page or file to which access was sought, the terms entered in the search fields, the time of access, the quantity of data transferred, an indication of whether access was successful, and the IP address of the computer from which access was sought.  
15      IP addresses are series of digits assigned to networked computers to facilitate their communication over the internet. When a website is accessed, the IP address of the computer seeking access is communicated to the server on which the website consulted is stored. That connection is necessary so that the data accessed maybe transferred to the correct recipient.   
16      Furthermore, it is clear from the order for the reference and the documents before the Court that internet service providers allocate to the computers of internet users either a ‘static’ IP address or a ‘dynamic’ IP address, that is to say an IP address which changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider.  
17      Mr Breyer brought an action before the German administrative courts seeking an order restraining the Federal Republic of Germany from storing, or arranging for third parties to store, after consultation of the websites accessible to the public run by the German Federal institutions’ online media services, the IP address of the applicant’s host system except in so far as its storage is unnecessary in order to restore the availability of those media in the event of a fault occurring.  
18      Since Mr Breyer’s action at first instance was dismissed, he brought an appeal against that decision.  
19      The court of appeal varied that decision in part. It ordered the Federal Republic of Germany to refrain from storing or arranging for third parties to store, at the end of each consultation period, the IP address of the host system from which Mr Breyer sought access, which was transmitted when he consulted publicly accessible websites of the German Federal institutions’ online media, where that address is stored together with the date of the consultation period to which it relates and where Mr Breyer has revealed his identity during that use, including in the form of an electronic address mentioning his identity, except in so far as that storage is not necessary in order to restore the dissemination of those media in the event of a fault occurring.  
20      According to the court of appeal, a dynamic IP address, together with the date on which the website was accessed to which that address relates constitutes, if the user of the website concerned has revealed his identity during that consultation period, personal data, because the operator of that website is able to identify the user by linking his name to his computer’s IP address.  
21      However, the court of appeal held that Mr Breyer’s action could not be upheld in other situations. If Mr Breyer does not reveal his identity during a consultation period, only the internet service provider could connect the IP address to an identified subscriber. However, in the hands of the Federal Republic of Germany, in its capacity as provider of online media services, the IP address is not personal data, even in combination with the date of the consultation period to which it relates, because the user of the websites concerned is not identifiable by that Member State.  
22      Mr Breyer and the Federal Republic of Germany each brought an appeal on a point of law before the Bundesgerichtshof (Federal Court of Justice, Germany) against the decision of the appeal court. Mr Breyer sought to have his application for an injunction upheld in its entirety. The Federal Republic of Germany sought to have it dismissed.  
23      The referring court states that the dynamic IP addresses of Mr Breyer’s computer stored by the Federal Republic of Germany, acting in its capacity as an online media services provider, are, at least in the context of other data stored in daily files, specific data on Mr Breyer’s factual circumstances, given that they provide information relating to his use of certain websites or certain internet files on certain dates.   
24      Nevertheless, the data stored does not enable Mr Breyer to be directly identified. The operators of the websites at issue in the main proceedings can identify Mr Breyer only if the information relating to his identity is communicated to them by his internet service provider. The classification of those data as ‘personal data’ thus depends on whether Mr Breyer is identifiable.  
25      The Bundesgerichtshof (Federal Court of Justice) refers to the academic disagreement relating to whether, in order to determine whether someone is identifiable, an ‘objective’ or ‘relative’ criterion must be used. The application of an ‘objective’ criterion would have the consequence that data such as the IP addresses at issue in the main proceedings may be regarded, at the end of the period of use of the websites at issue, as being personal data even if only a third party is able to determine the identity of the data subject, that third party being, in the present case, Mr Breyer’s internet service provider, which stored the additional data enabling his identification by means of those IP addresses. According to a ‘relative’ criterion, such data may be regarded as personal data in relation to an entity such as Mr Breyer’s internet service provider because they allow the user to be precisely identified (see, in that connection, judgment of 24 November 2011,   
Scarlet Extended  
, C-70/10, EU:C:2011:771, paragraph 51), but not being regarded as such with respect to another entity, since that operator does not have, if Mr Breyer has not disclosed his identity during the consultation of those websites, the information necessary to identify him without disproportionate effort.  
26      If the dynamic IP addresses of Mr Breyer’s computer, together with the date of the relevant consultation period, were to be considered as constituting personal data, the referring court asks whether the storage of those IP addresses at the end of that consultation period is authorised by Article 7(f) of that directive.  
27      In that connection, the Bundesgerichtshof (Federal Court of Justice) states, first, that under Paragraph 15(1) of the TMG, online media services providers may collect and use the personal data of a user only to the extent that that is necessary to facilitate and charge for the use of those media. Second, the referring court states that, according to the Federal Republic of Germany, storage of those data is necessary to guarantee the security and continued proper functioning of the online media services that it makes accessible to the public, in particular, enabling cyber attacks known as ‘denial-of-service’ attacks, which aim to paralyse the functioning of the sites by the targeted and coordinated saturation of certain web servers with huge numbers of requests, to be identified and combated.  
28      According to the referring court, if and to the extent it is necessary for the online media services provider to take measures to combat such attacks, those measures may be regarded as necessary to ‘facilitate … the use of telemedia’ pursuant to Paragraph 15 of the TMG. However, academic opinion mostly supports the view, first, that the collection and use of personal data relating to the user of a website is authorised only in order to facilitate the specific use of that website and, second, that those data must be deleted at the end of period of consultation concerned if they are not data required for billing purposes. Such a restrictive reading of Paragraph 15(1) of the TMG would prevent the storage of IP addresses from being authorised in order to guarantee in a general manner the security and continued proper functioning of online media.  
29      The referring court asks whether that interpretation, which is the interpretation advocated by the court of appeal, is in accordance with Article 7(f) of Directive 95/46, having regard, in particular with the criteria laid down by the Court in paragraph 29 et seq. of the judgment of 24 November 2011,   
ASNEF and FECEMD  
 (C-468/10 and C-469/10, EU:C:2011:777).  
30      In those circumstances the Bundesgerichtshof (Federal Court of Justice) decided to stay the proceedings before it and to refer the following questions to the Court for a preliminary ruling:   
‘(1)      Must Article 2(a) of Directive 95/46 … be interpreted as meaning that an internet protocol address (IP address) which an [online media] service provider stores when his website is accessed already constitutes personal data for the service provider if a third party (an access provider) has the additional knowledge required in order to identify the data subject?  
(2)      Does Article 7(f) of [that directive] preclude a provision in national law under which a service provider may collect and use a user’s personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the telemedium by the user concerned, and under which the purpose of ensuring the general operability of the telemedium cannot justify use of the data beyond the end of the particular use of the telemedium?’  
   
Consideration of the questions referred for a preliminary ruling  
   
The first question  
31      By its first question, the referring court asks essentially whether Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that that provider makes accessible to the public constitutes, with regard to that service provider, personal data within the meaning of that provision, where, only a third party, in the present case the internet service provider, has the additional data necessary to identify him.  
32      According to that provision, ‘personal data’ ‘mean any information relating to an identified or identifiable natural person (“data subject”)’. Pursuant to that provision, an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.  
33      As a preliminary point, it must be noted that, in paragraph 51 of the judgment of 24 November 2011,   
Scarlet Extended  
 (C-70/10, EU:C:2011:771), which concerned inter alia the interpretation of the same directive, the Court held essentially that the IP addresses of internet users were protected personal data because they allow users to be precisely identified.  
34      However, that finding by the Court related to the situation in which the collection and identification of the IP addresses of internet users is carried out by internet service providers.  
35      In the present case, the first question concerns the situation in which it is the online media services provider, namely the Federal Republic of Germany, which registers IP addresses of the users of a website that it makes accessible to the public, without having the additional data necessary in order to identify those users.  
36      Furthermore, it is common ground that the IP addresses to which the national court refers are ‘dynamic’ IP addresses, that is to say provisional addresses which are assigned for each internet connection and replaced when subsequent connections are made, and not ‘static’ IP addresses, which are invariable and allow continuous identification of the device connected to the network.  
37      The referring court’s first question is based therefore on the premiss, first, that data consisting in a dynamic IP address and the date and time that a website was accessed from that IP address registered by an online media services provider do not, without more, give the service provider the possibility to identify the user who consulted that website during that period of use and, second, the internet services provider has additional data which, if combined with the IP address would enable the user to be identified.  
38      In that connection, it must be noted, first of all, that it is common ground that a dynamic IP address does not constitute information relating to an ‘identified natural person’, since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer.  
39      Next, in order to determine whether, in the situation described in paragraph 37 of the present judgment, a dynamic IP address constitutes personal data within the meaning of Article 2(a) of Directive 96/45 in relation to an online media services provider, it must be ascertained whether such an IP address, registered by such a provider, may be treated as data relating to an ‘identifiable natural person’ where the additional data necessary in order to identify the user of a website that the services provider makes accessible to the public are held by that user’s internet service provider.  
40      In that connection, it is clear from the wording of Article 2(a) of Directive 95/46 that an identifiable person is one who can be identified, directly or indirectly.  
41      The use by the EU legislature of the word ‘indirectly’ suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified.  
42      Furthermore, recital 26 of Directive 95/46 states that, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.  
43      In so far as that recital refers to the means likely reasonably to be used by both the controller and by ‘any other person’, its wording suggests that, for information to be treated as ‘personal data’ within the meaning of Article 2(a) of that directive, it is not required that all the information enabling the identification of the data subject must be in the hands of one person.  
44      The fact that the additional data necessary to identify the user of a website are held not by the online media services provider, but by that user’s internet service provider does not appear to be such as to exclude that dynamic IP addresses registered by the online media services provider constitute personal data within the meaning of Article 2(a) of Directive 95/46.  
45      However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject.  
46      Thus, as the Advocate General stated essentially in point 68 of his Opinion, that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.  
47      Although the referring court states in its order for reference that German law does not allow the internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however, subject to verifications to be made in that regard by the referring court that, in particular, in the event of cyber attacks legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.  
48      Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.  
49      Having regard to all the foregoing considerations, the answer to the first question is that Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.  
   
The second question  
50      By its second question, the referring court asks essentially whether Article 7(f) of Directive 95/46 must be interpreted as precluding the legislation of a Member State under which an online media services provider may collect and use a user’s personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of those services by the user concerned, and under which the purpose of ensuring the general operability of those services cannot justify use of the data beyond the end of the particular use of them.  
51      Before answering that question, it must be determined whether the processing of personal data at issue in the main proceedings, that is dynamic IP addresses of users of certain websites of the German Federal institutions, is excluded from the scope of Directive 95/46 under Article 3(2), first indent thereof, pursuant to which that directive does not apply to personal data processing operations concerning, in particular, the activities of the State in areas of criminal law.  
52      In that connection, it must be recalled that the activities mentioned by way of examples by that provision are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals (see judgments of 6 November 2003,   
Lindqvist  
, C-101/01, EU:C:2003:596, paragraph 43, and of 16 December 2008,   
Satakunnan Markkinapörssi and Satamedia  
, C-73/07, EU:C:2008:727, paragraph 41).  
53      In the present case, subject to verifications to be made in that regard by the referring court, it appears that the German Federal institutions, which provide the online media services and which are responsible for the processing of dynamic IP addresses act, in spite of their status as public authorities, as individuals and outside the activities of the State in the area of criminal law.  
54      Therefore, it must be determined whether the legislation of a Member State, such as that at issue in the main proceedings, is compatible with Article 7(f) of Directive 95/46.  
55      To that end, it is important to recall that the national legislation at issue in the main proceedings, as interpreted in the restrictive sense described by the referring court, authorises the collection and use of personal data relating to a user of those services, without his consent, only to the extent that is necessary to facilitate and charge for the specific use of online media by the user concerned, even though the objective aiming to ensure the general capacity relating to the functioning of the online media may justify the use of those data at the end of that period of use of such media.  
56      Pursuant to Article 7(f) of Directive 95/46, personal data may be processed if ‘processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)’ of the Directive.   
57      The Court has held that Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful and that the Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article (see, to that effect, judgment of 24 November 2011,   
ASNEF and FECEMD  
, C-468/10 and C-469/10, EU:C:2011:777, paragraphs 30 and 32).  
58      Article 5 of Directive 95/46 authorises Member States to specify, within the limits of Chapter II of that directive and, accordingly, Article 7 thereof, the conditions under which the processing of personal data is lawful, the margin of discretion which Member States have pursuant to Article 5 can therefore be used only in accordance with the objective pursued by that directive of maintaining a balance between the free movement of personal data and the protection of private life. Under Article 5 of Directive 95/46, Member States also cannot introduce principles relating to the lawfulness of the processing of personal data other than those listed in Article 7 thereof, nor can they amend, by additional requirements, the scope of the six principles provided for in Article 7 (see, to that effect, judgment of 24 November 2011,   
ASNEF and FECEMD  
, C-468/10 and C-469/10, EU:C:2011:777, paragraphs 33, 34 and 36).  
59      In the present case, it appears that Paragraph 15 of the TMG, if it were interpreted in the strict manner mentioned in paragraph 55 of the present judgment, has a more restrictive scope than that of the principle laid down in Article 7(f) of Directive 95/46.   
60      Whereas Article 7(f) of that directive refers, in a general manner, to ‘the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed’, Paragraph 15 of the TMG authorises the service provider to collect and use personal data of a user only in so far as that is necessary in order to facilitate, and charge for, the particular use of electronic media. Therefore, Paragraph 15 of the TMG precludes the storage of personal data, after the consultation of online media, in a general manner in order to guarantee the use of those media. The German Federal institutions, which provide online media services, may also have a legitimate interest in ensuring, in addition to the specific use of their publicly accessible websites, the continued functioning of those websites.  
61      Thus, as the Advocate General pointed out, in points 100 and 101 of his Opinion, such national legislation goes further than defining the notion of ‘legitimate interests’ in Article 7(f) of Directive 95/46, in accordance with Article 5 of Directive 95/46.  
62      Article 7(f) of that directive precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case. Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case (see, to that effect, judgment of 24 November 2011,   
ASNEF and FECEMD  
, C-468/10 and C-469/10, EU:C:2011:777, paragraphs 47 and 48).  
63      As regards the processing of personal data of the users of online media websites, legislation, such as that at issue in the main proceedings, reduces the scope of the principle laid down in Article 7(f) of Directive 95/46 by excluding the possibility to balance the objective of ensuring the general operability of the online media against the interests or fundamental rights and freedoms of those users which, in accordance with that provision, calls for protection under Article 1(1) of that directive.  
64      It follows from all of the foregoing considerations that the answer to the second question is that Article 7(f) of Directive 95/46 must be interpreted as meaning that it precludes the legislation of a Member State under which an online media services provider may collect and use personal data relating to a user of those service, without his consent, only in so far as the collection and use of that information are necessary to facilitate and charge for the specific use of those services by that user, even though the objective aiming to ensure the general operability of those services may justify the use of those data after consultation of those websites.  
   
Costs  
65      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Second Chamber) hereby rules:  
1.        
Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.  
2.        
Article 7(f) of Directive 95/46 must be interpreted as precluding the legislation of a Member State, pursuant to which an online media services provider may collect and use personal data relating to a user of those services, without his consent, only in so far as that the collection and use of that data are necessary to facilitate and charge for the specific use of those services by that user, even though the objective aiming to ensure the general operability of those services may justify the use of those data after a consultation period of those websites.

ID: f373eaa2-f3ff-41ae-afbf-d2c96504c2e8

Judgment of 5 May 2011, C-543/09 (  
Deutsche Telekom  
)  
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Directories of subscribers   
General data protection law   
 >   
Chapter II - Principles   
 >   
Lawfulness - Consent   
   
JUDGMENT OF THE COURT (Third Chamber)  
5 May 2011 (\*)  
(Electronic communications – Directive 2002/22/EC – Article 25(2) – Directive 2002/58/EC – Article 12 – Provision of directory enquiry services and directories – Obligation placed on an undertaking assigning telephone numbers to pass to other undertakings data in its possession relating to the subscribers of third-party undertakings)  
In Case C-543/09,  
REFERENCE for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Germany), made by decision of 28 October 2009, received at the Court on 22 December 2009, in the proceedings  
Deutsche Telekom AG  
v  
Bundesrepublik Deutschland,  
intervening parties:  
GoYellow GmbH,  
Telix AG,  
THE COURT (Third Chamber),  
composed of K. Lenaerts (Rapporteur), President of the Chamber, R. Silva de Lapuerta, G. Arestis, J. Malenovský and T. von Danwitz, Judges,  
Advocate General: V. Trstenjak,  
Registrar: K. Malacek, Administrator,  
having regard to the written procedure and further to the hearing on 2 December 2010,  
after considering the observations submitted on behalf of:  
–        Deutsche Telekom AG, by W. Roth, Rechtsanwalt, and I. Fink, Justitiarin,  
–        the Bundesrepublik Deutschland, by E. Greiwe, acting as Agent,  
–        GoYellow GmbH, by G. Jochum, Rechtsanwalt,  
–        the Italian Government, by G. Palmieri, acting as Agent, and by P. Gentili, avvocato dello Stato,  
–        the United Kingdom Government, by F. Penlington and C. Murrell, acting as Agents, and by T. Ward, Barrister,  
–        the European Commission, by A. Nijenhuis and G. Braun, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 17 February 2011,  
gives the following  
Judgment  
1        This reference for a preliminary ruling concerns the interpretation of Article 25(2) of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users’ rights relating to electronic communications networks and services (Universal Service Directive) (OJ 2002 L 108, p. 51) and of Article 12 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).  
2        The reference has been made in proceedings between, on the one hand, Deutsche Telekom AG (‘Deutsche Telekom’) and, on the other, the Federal Republic of Germany, represented by the Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Agency for Electricity, Gas, Telecommunications, Post and Rail Networks) (‘the Bundesnetzagentur’) concerning the obligation, imposed by the Telekommunikationsgesetz (German Law on Telecommunications) (‘TKG’), on undertakings which assign telephone numbers to make available, to other undertakings whose activity consists in providing publicly available directory enquiry services and directories, data in their possession relating to subscribers of third-party undertakings.  
   
Legal context  
   
European Union (‘EU’) legislation  
 Directive 95/46/EC  
3        Article 1(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) states that that directive is aimed at protecting the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data.  
4        Article 2(h) of Directive 95/46 defines ‘the data subject’s consent’ as being ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’.  
5        Article 7(a) of that directive provides that personal data may be processed if ‘the data subject has unambiguously given his consent’.  
 The ONP Directive  
6        As from 1 January 1998, the provision of telecommunications services and infrastructures was liberalised in the European Union. That liberalisation coincided with the establishment of a harmonised regulatory framework which included Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment (OJ 1998 L 101, p. 24; ‘the ONP Directive’).  
7        The ONP Directive was repealed by Article 26 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ 2002 L 108, p. 33). Article 6(3) of the ONP Directive provided:  
‘In order to ensure provision of [directory and directory enquiry services], Member States shall ensure that all organisations which assign telephone numbers to subscribers meet all reasonable requests to make available the relevant information in an agreed format on terms which are fair, cost oriented and non-discriminatory.’  
 The common regulatory framework  
8        As is stated in recital 1 in the preamble to the Framework Directive, a few years after the liberalisation of the telecommunications markets, the conditions for effective competition had been created and a common regulatory framework (‘CRF’) had been adopted. The CRF includes the Framework Directive, the Universal Service Directive and also the Directive on privacy and electronic communications.  
–       The Framework Directive  
9        Article 1(1) of the Framework Directive states:  
‘This Directive establishes a harmonised framework for the regulation of electronic communications services … It lays down tasks of national regulatory authorities and establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the Community.’  
10      The Framework Directive gives national regulatory authorities (‘NRAs’) specific tasks for regulating electronic communications markets. Thus, under Article 16 of that directive, the NRAs are to carry out an analysis of the relevant markets in the electronic communications sector and to determine whether those markets are effectively competitive. If a market is not effectively competitive, the competent NRA is to impose specific regulatory obligations on undertakings with significant power on that market.  
–       The Universal Service Directive  
11      Recitals 11 and 35 to the Universal Service Directive state:  
‘(11) Directory information and a directory enquiry service constitute an essential access tool for publicly available telephone services and form part of the universal service obligation. Users and consumers desire comprehensive directories and a directory enquiry service covering all listed telephone subscribers and their numbers (including fixed and mobile numbers) and want this information to be presented in a non-preferential fashion. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [OJ 1998 L 24, p. 1] ensures the subscribers’ right to privacy with regard to the inclusion of their personal information in a public directory.   
…  
(35)      The provision of directory enquiry services and directories is already open to competition. The provisions of this Directive complement the provisions of Directive 97/66/EC by giving subscribers a right to have their personal data included in a printed or electronic directory. All service providers which assign telephone numbers to their subscribers are obliged to make relevant information available in a fair, cost-oriented and non-discriminatory manner.’  
12      Article 5 of the Universal Service Directive, which is entitled ‘Directory enquiry services and directories’, provided, in the version in force at the material time:  
‘1.      Member States shall ensure that:  
(a)      at least one comprehensive directory is available to end-users in a form approved by the relevant authority, whether printed or electronic, or both, and is updated on a regular basis, and at least once a year;  
(b)      at least one comprehensive telephone directory enquiry service is available to all end-users, including users of public pay telephones.  
2.      The directories in paragraph 1 shall comprise, subject to the provisions of Article 11 of Directive 97/66/EC, all subscribers of publicly available telephone services.  
…’  
13      Under Article 17 of the Universal Service Directive, the NRAs – after carrying out a retail market analysis and after determining that the relevant market is not effectively competitive – are to impose appropriate regulatory obligations on undertakings identified as having significant market power.  
14      Article 25 of the Universal Service Directive, which is entitled ‘Operator assistance and directory enquiry services’, provided, in the version in force at the material time:  
‘1.      Member States shall ensure that subscribers to publicly available telephone services have the right to have an entry in the publicly available directory referred to in Article 5(1)(a).  
2.      Member States shall ensure that all undertakings which assign telephone numbers to subscribers meet all reasonable requests to make available, for the purposes of the provision of publicly available directory enquiry services and directories, the relevant information in an agreed format on terms which are fair, objective, cost-oriented and non-discriminatory.  
…  
5.      Paragraphs 1, 2 … apply subject to the requirements of Community legislation on the protection of personal data and privacy and, in particular, Article 11 of Directive 97/66/EC.’  
–       The Directive on privacy and electronic communications  
15      Recitals 38 and 39 to the Directive on privacy and electronic communications state:  
‘(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.  
(39)      The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.’  
16      Under paragraphs 1 to 3 of Article 12 of the Directive on privacy and electronic communications, which is entitled ‘Directories of subscribers’:  
‘1.      Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.   
2.      Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.  
3.      Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.’  
17      Article 19 of the Directive on privacy and electronic communications repealed Directive 97/66 with effect from 31 October 2003 and provided that ‘[r]eferences made to the repealed Directive shall be construed as being made to this Directive’. References to Article 11 of Directive 97/66 must therefore be construed as being references to Article 12 of the Directive on privacy and electronic communications.  
   
National legislation  
18      According to the Bundesverwaltungsgericht, under Paragraphs 47(1), 104 and 105 of the TKG, read in conjunction, any undertaking which assigns telephone numbers to end-users is under an obligation to pass on to providers of publicly available directory enquiry services and directories who so request not only data relating to its own subscribers, but also data in its possession relating to subscribers of third-party service providers. The passing on of such data is not conditional on the consent, or lack of objection, of the subscribers concerned or their telephone service providers.  
   
Facts and the questions referred for a preliminary ruling  
19      In its capacity as a telecommunications network operator in Germany, Deutsche Telekom assigns telephone numbers to its subscribers. It operates a nationwide telephone directory enquiry service. It also publishes printed and electronic directories containing data relating not only to its own customers, but also to subscribers of other undertakings. Deutsche Telekom acquires the data necessary for those purposes from the telephone service providers which assigned the telephone numbers to the subscribers concerned. In this way, it has concluded contracts for the acquisition of subscriber data with approximately 100 undertakings.  
20      GoYellow GmbH (‘GoYellow’) and Telix AG (‘Telix’) – the interveners in the main proceedings – operate an internet enquiry service and a telephone directory enquiry service, respectively. They use data made available to them by Deutsche Telekom in return for payment. Following a disagreement as to the scope of the data which Deutsche Telekom was under an obligation to pass on to GoYellow and Telix, the latter companies brought the matter before the Bundesnetzagentur pursuant to Paragraphs 47(1), 104 and 105 of the TKG.  
21      By decision of 11 September 2006, the Bundesnetzagentur ordered Deutsche Telekom to make available to GoYellow and Telix not only the data relating to Deutsche Telekom’s own subscribers but also the data in its possession relating to the subscribers of third-party telephone service providers (‘the external data’), even where those providers or their subscribers wished those data to be published only by Deutsche Telekom.  
22      Deutsche Telekom brought an action before the Verwaltungsgericht Köln (Administrative Court, Cologne) against that decision of the Bundesnetzagentur.  
23      By judgment of 14 February 2008, the Verwaltungsgericht Köln dismissed the action. Deutsche Telekom then appealed on a point of law to the Bundesverwaltungsgericht (Federal Administrative Court), submitting inter alia that an obligation to pass on data which encompasses external data infringes the Universal Service Directive.  
24      In the order for reference, the Bundesverwaltungsgericht explains that the dispute in the main proceedings is limited, on the one hand, to the obligation imposed on Deutsche Telekom to pass external data on to GoYellow and Telix and, on the other, to the data which the subscriber or his provider wishes to see published only by Deutsche Telekom. The Bundesverwaltungsgericht states that, on the basis of national law alone, the appeal on a point of law falls to be dismissed. It wonders, however, whether the obligation imposed by the national law applicable to the dispute before it is in conformity with EU law.  
25      The Bundesverwaltungsgericht observes, first, that the judgment in Case C-109/03   
KPN Telecom  
 [2004] ECR I-11273 confirms that Article 25(2) of the Universal Service Directive requires an undertaking which assigns telephone numbers to pass on only data relating to its own subscribers. Secondly, accordingly to the Bundesverwaltungsgericht, the possibility cannot be ruled put that – in the light, inter alia, of the general purpose of the Framework Directive, which is to promote competition – EU law allows the national legislature to extend the obligation so as to make external data available. According to the Bundesverwaltungsgericht, gathering data from a single party is likely to forestall the significant impediments normally associated with procuring data from each individual undertaking which assigns telephone numbers when lists of data necessary for the provision of directory and directory enquiry services are established and especially when they are regularly updated; it is also likely to promote, on a lasting basis, strong competitive structures.  
26      If it should transpire that the national legislature is justified in extending the scope of the obligation to make data available so that it covers external data held by the undertaking subject to that obligation, the Bundesverwaltungsgericht is uncertain as to whether Article 12 of the Universal Service Directive makes the passing on of that external data conditional on the consent of the subscribers concerned and of their telephone service provider.  
27      In those circumstances, the Bundesverwaltungsgericht decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:  
‘1.      Must Article 25(2) of Directive 2002/22/EC of [the Universal Service Directive] be interpreted as meaning that Member States may require undertakings which assign telephone numbers to subscribers to make available data relating to subscribers to whom the undertaking in question has not itself assigned telephone numbers for the purpose of the provision of publicly available directory enquiry services and directories, in so far as that undertaking has such data in its possession?   
2.      If the answer to the previous question is in the affirmative:  
Must Article 12 of Directive 2002/58/EC of the [Directive on privacy and electronic communications] be interpreted as meaning that the imposition of the abovementioned obligation by the national legislature is conditional upon the consent of, or at least the lack of any objection by, the other telephone service provider or its subscribers to the passing on of the data?’  
   
Consideration of the questions referred  
   
The first question  
28      By its first question, the Bundesverwaltungsgericht asks, in essence, whether Article 25(2) of the Universal Service Directive must be interpreted as precluding national legislation which places undertakings assigning telephone numbers to end-users under an obligation to make available, to undertakings whose activity consists in providing publicly available directory enquiry services and directories, data in their possession relating to subscribers of third-party undertakings.  
29      In order to answer that question, it is appropriate first to consider whether the external data at issue in the dispute in the main proceedings is ‘relevant information’ for the purposes of Article 25(2) of the Universal Service Directive, which undertakings assigning telephone numbers are required, under that provision, to pass on to undertakings whose activity consists in providing publicly available directory enquiry services and directories.  
30      In that regard, it should be noted that, under Article 25(2) of the Universal Service Directive, an obligation to pass on data is imposed only on ‘undertakings which assign telephone numbers to subscribers’. Given the link thus established between, on the one hand, that obligation to pass on data and, on the other, the assignment of a telephone number to a subscriber, it must be held that the ‘relevant information’ the communication of which is required under Article 25(2) of the Universal Service Directive concerns solely the data relating to the subscribers of the undertakings concerned: such a provision imposes an obligation on an undertaking, such as Deutsche Telekom, in its capacity as an undertaking which assigns telephone numbers and not in its capacity as a provider of directory enquiry services and directories.  
31      That interpretation is borne out by the objective pursued by Article 25(2) of the Universal Service Directive, which is to ensure compliance with the obligation of universal service as laid down in Article 5(1) of that directive, under which Member States are to ensure that at least one comprehensive directory or one comprehensive telephone directory enquiry service is made available to end-users. An obligation imposed on each undertaking which assigns telephone numbers to pass on data relating to its own subscribers enables the undertaking designated to provide the universal service in question to establish an exhaustive data base and, therefore, to ensure compliance with the obligation under Article 5(1).  
32      In support of their argument that the obligation under Article 25(2) of the Universal Service Directive to pass on data also encompasses external data, the Bundesnetzagentur and the Italian Government refer to recital 11 to that directive and to the CRF’s general objective of promoting competition.  
33      In that regard, it should be borne in mind that recital 11 to the Universal Service Directive states that ‘[u]sers and consumers desire comprehensive directories and a directory enquiry service covering all listed telephone subscribers and their numbers …’. That recital must, however, be read in conjunction with the universal service obligation laid down in Article 5(1) of that directive, which does not require the Member States to ensure that all directories and telephone directory enquiry services are comprehensive. Under that provision, the Member States must ensure only that at least one comprehensive directory or one comprehensive telephone directory enquiry service is made available to end-users. As is apparent from paragraph 31 above, an obligation to pass on data which applies to undertakings assigning telephone numbers and which covers only data relating to their own subscribers is sufficient to ensure compliance with the universal service obligation under Article 5(1).  
34      Nor does the CRF’s general objective, which is to promote competition, support the view that an undertaking assigning telephone numbers to subscribers, such as Deutsche Telekom, is required under Article 25(2) of the Universal Service Directive to pass on to third-party undertakings data other than data relating to its own subscribers.  
35      Article 25(2) of the Universal Service Directive must be interpreted in the light of its specific objective, which is to ensure compliance with the universal service obligation laid down in Article 5(1) of that directive.  
36      Moreover, recital 35 to the Universal Service Directive states that the provision of directory enquiry services and directories is already open to competition. In a competitive market, the obligation under Article 25(2) of that directive for undertakings which assign telephone numbers to pass on data relating to their own subscribers in principle not only enables the designated undertaking to ensure compliance with the universal service obligation laid down in Article 5(1) of that directive, but also enables any provider of telephone services to establish an exhaustive data base and to become active in the market for telephone directory enquiry services and directories. In that connection, it is sufficient that the provider concerned ask each undertaking assigning telephone numbers for the relevant data relating to its subscribers.  
37      It follows from the foregoing that the ‘relevant information’ for the purposes of Article 25(2) of the Universal Service Directive, the communication of which is required under that provision, encompasses only information which relates to the subscribers of the undertakings assigning telephone numbers.  
38      Secondly, it must be determined whether Article 25(2) of the Universal Service Directive undertakes full harmonisation or whether, on the contrary, that provision allows the Member States to impose on undertakings assigning telephone numbers an obligation to pass on to undertakings which intend to provide publicly available directory enquiry services and directories not only ‘relevant information’ for the purposes of that provision, but also external data.  
39      In that regard, it should be borne in mind from the outset that, in paragraph 35 of its judgment in   
KPN Telecom  
, concerning the interpretation of Article 6(3) of the ONP Directive, the content of which is similar to that of Article 25(2) of the Universal Service Directive, the Court held that Article 6(3) did not seek to effect full harmonisation and that the Member States retained competence for determining whether in a specific national context certain additional data ought to be made available to third parties.  
40      Deutsche Telekom maintains, however, as do the United Kingdom Government and the European Commission, that Article 25(2) of the Universal Service Directive cannot be interpreted in that way, since it is part of the CRF, which – as is stated in Article 1(1) of the Framework Directive – is a harmonised framework for the regulation of electronic communications services. Accordingly, the national legislature may not impose on the undertakings concerned obligations which go beyond those laid down in Article 25(2).  
41      In that regard, it should first be observed that Article 25(2) of the Universal Service Directive is part of Chapter IV of that directive, which concerns end-user interests and rights. Yet the Court has held that the Framework Directive and the Universal Service Directive do not provide for full harmonisation of consumer-protection aspects (Case C-522/08   
Telekomunikacja Polska   
[2010] ECR I-0000, paragraph 29).  
42      Secondly, it should be borne in mind that Article 25(2) of the Universal Service Directive is aimed at ensuring compliance with the obligation, placed on the Member States under Article 5(1) of that directive, to ensure that at least one comprehensive directory or one comprehensive telephone directory enquiry service is made available to end-users. Since that marks a minimum requirement which the Member States must satisfy, in principle they remain free to adopt more stringent provisions in order to facilitate the entry of new traders on the market for publicly available telephone and directory services.  
43      Thus, the CRF does not preclude national legislation such as that at issue in the main proceedings, which, being directed at any undertaking which assigns telephone numbers to end-users, affects electronic communications undertakings in a general and non-discriminatory manner – provided, however, that such legislation does not encroach upon the powers which the NRAs derive directly from the provisions of the CRF (  
Telekomunikacja Polska  
, paragraphs 27 and 28; see also Case C-424/07   
Commission  
 v   
Germany  
 [2009] ECR I-11431, paragraphs 78 and 91 to 99).  
44      In the present case, it must be held that national legislation such as that at issue in the main proceedings does not affect any of the powers expressly conferred by the CRF on the NRA concerned.  
45      First, Article 25(2) of the Universal Service Directive does not confer any specific powers or impose any specific obligations on the NRAs. That provision imposes obligations only on the Member States as such.  
46      Secondly, national legislation such as that at issue in the main proceedings does not in any way affect the powers of the NRA concerned, arising under Article 16 of the Framework Directive and Article 17 of the Universal Service Directive, relating to the analysis of the various electronic communications markets and the imposition of regulatory obligations on undertakings with significant market power on markets which are not effectively competitive. None the less, the mere fact that, if the undertakings concerned comply with the national legislation at issue in the main proceedings, the NRA will no longer need, after any analysis it may carry out of the retail market concerned, to take any specific measures – that is to say, to require undertakings with significant market power to pass on external data to third-party undertakings – does not support the inference that the powers which the NRA concerned derives from Article 17 of the Universal Service Directive are directly affected (see, by analogy, as regards a general prohibition of tied sales,   
Telekomunikacja Polska  
, paragraph 28).  
47      It follows from all the foregoing that the answer to the first question is that Article 25(2) of the Universal Service Directive must be interpreted as not precluding national legislation under which undertakings assigning telephone numbers to end-users must make available to undertakings whose activity consists in providing publicly available directory enquiry services and directories not only data relating to their own subscribers but also data in their possession relating to subscribers of third-party undertakings.  
   
The second question  
48      By its second question, the Bundesverwaltungsgericht asks, in essence, whether Article 12 of the Directive on privacy and electronic communications makes the passing on, to an undertaking whose activity consists in providing publicly available directory enquiry services and directories, by an undertaking which assigns telephone numbers, of data in its possession relating to subscribers of a third-party undertaking conditional on the consent, or lack of objection, of that undertaking or its subscribers.  
49      In that regard, it should be noted that Article 8(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’) states that ‘[e]veryone has the right to the protection of personal data concerning him or her’.  
50      Directive 95/46 is designed to ensure, in the Member States, observance of the right to protection of personal data. As is clear from Article 1(2) thereof, the Directive on privacy and electronic communications clarifies and supplements Directive 95/46 in the electronic communications sector.  
51      However, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society (Joined Cases C-92/09 and C-93/09   
Volker und Markus Schecke and Eifert  
 [2010] ECR I-0000, paragraph 48 and the case-law cited).  
52      Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied. It provides that personal data ‘must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.  
53      The passing of subscribers’ personal data to a third-party undertaking which intends to provide publicly available directory enquiry services and directories constitutes processing of personal data for the purposes of Article 8(2) of the Charter, which may be undertaken only ‘on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.  
54      Moreover, the Directive on privacy and electronic communications makes it clear that that directive makes the publication, in printed or electronic directories, of personal data concerning subscribers conditional on the consent of those subscribers.  
55      Thus, Article 12(2) of that directive provides that subscribers are to be free to decide whether their personal data is to be included in a public directory and, if so, which personal data.  
56      On the other hand, there is no provision in the Directive on privacy and electronic communications which makes the publication of personal data relating to subscribers conditional on any consent from the undertaking which assigned the telephone numbers concerned or which has external data in its possession. Such an undertaking cannot, in its own right, rely on the right of prior consent, which is conferred solely on subscribers.  
57      By its second question, the Bundesverwaltungsgericht also asks whether Article 12 of the Directive on privacy and electronic communications makes the passing of personal data to a third-party undertaking whose activity consists in providing publicly available directory enquiry services and directories conditional on renewed consent from the subscriber, where the subscriber has consented to the publication of his personal data in one directory only, in this case the directory drawn up by Deutsche Telekom.  
58      In that regard, it should be borne in mind from the outset that it is clear from Article 12(1) of the Directive on privacy and electronic communications and from recital 38 thereto that, before being included in public directories, subscribers are to be informed of the purposes of the directory and of any particular usage which may be made of it, in particular through search functions embedded in the software of the electronic versions of the directories. Such prior information gives the subscriber concerned the opportunity to give free, specific and informed consent, for the purposes of Articles 2(h) and 7(a) of Directive 95/46, to the publication of his personal data in public directories.  
59      Recital 39 to the Directive on privacy and electronic communications states, with respect to the obligation of prior information for subscribers under Article 12(1) of that directive: ‘[w]here the [personal] data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients’.  
60      However, after obtaining the information referred to in Article 12(1) of that directive, the subscriber may – as is clear from Article 12(2) – decide only whether his personal data may be included in a public directory and, if so, which personal data.  
61      As the Advocate General observed in point 122 of her Opinion, it follows from a contextual and systematic interpretation of Article 12 of the Directive on privacy and electronic communications that the consent under Article 12(2) relates to the purpose of the publication of personal data in a public directory and not to the identity of any particular directory provider.  
62      First, the wording of Article 12(2) of the Directive on privacy and electronic communications does not support the inference that the subscriber has a selective right to decide in favour of certain providers of publicly available directory enquiry services and directories. It should be noted in that regard that it is the publication itself of the personal data in a public directory with a specific purpose which may turn out to be detrimental for a subscriber. Where, however, the subscriber has consented to his data being published in a directory with a specific purpose, he will generally not have standing to object to the publication of the same data in another, similar directory.  
63      Secondly, recital 39 to that directive confirms that the passing of subscribers’ personal data to third parties is ‘subject to the condition that the data may not be used for other purposes than those for which they were collected’.  
64      Thirdly, the Directive on privacy and electronic communications refers to a situation in which provision can be made for the subscriber’s renewed or specific consent. Thus, under Article 12(3) of that directive, Member States may require that, for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers. Recital 39 to that directive states that renewed consent should be obtained from the subscriber ‘[i]f the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose’.  
65      It follows that, where a subscriber has been informed by the undertaking which assigned him a telephone number of the possibility that his personal data may be passed to a third-party undertaking, such as Deutsche Telekom, with a view to being published in a public directory, and where he has consented to the publication of those data in such a directory (in the present case, Deutsche Telekom’s directory), renewed consent is not needed from the subscriber for the passing of those same data to another undertaking which intends to publish a printed or electronic public directory, or to make such directories available for consultation through directory enquiry services, if it is guaranteed that the data in question will not be used for purposes other than those for which the data were collected with a view to their first publication. The consent given under Article 12(2) of the Directive on privacy and electronic communications, by a subscriber who has been duly informed, to the publication of his personal data in a public directory relates to the purpose of that publication and thus extends to any subsequent processing of those data by third-party undertakings active in the market for publicly available directory enquiry services and directories, provided that such processing pursues that same purpose.  
66      Moreover, where a subscriber has consented to the passing of his personal data to a given undertaking with a view to their publication in a public directory of that undertaking, the passing of the same data to another undertaking intending to publish a public directory without renewed consent having been obtained from that subscriber is not capable of substantively impairing the right to protection of personal data, as recognised in Article 8 of the Charter.  
67      Consequently, the answer to the second question is that Article 12 of the Directive on privacy and electronic communications must be interpreted as not precluding national legislation under which an undertaking publishing public directories must pass personal data in its possession relating to subscribers of other telephone service providers to a third-party undertaking whose activity consists in publishing a printed or electronic public directory or making such directories obtainable through directory enquiry services and which does not make the passing on of those data conditional on renewed consent from the subscribers, provided, however, that those subscribers have been informed, before the first inclusion of their data in a public directory, of the purpose of that directory and of the fact that those data may be communicated to another telephone service provider and that it is guaranteed that those data will not, once passed on, be used for purposes other than those for which they were collected with a view to their first publication.  
   
Costs  
68      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Third Chamber) hereby rules:  
1.        
Article 25(2) of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users’ rights relating to electronic communications networks and services (Universal Service Directive) must be interpreted as not precluding national legislation under which undertakings assigning telephone numbers to end-users must make available to undertakings whose activity consists in providing publicly available directory enquiry services and directories not only data relating to their own subscribers but also data in their possession relating to subscribers of third-party undertakings.  
2.        
Article 12 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) must be interpreted as not precluding national legislation under which an undertaking publishing public directories must pass personal data in its possession relating to subscribers of other telephone service providers to a third-party undertaking whose activity consists in publishing a printed or electronic public directory or making such directories obtainable through directory enquiry services, and under which the passing on of those data is not conditional on renewed consent from the subscribers, provided, however, that those subscribers have been informed, before the first inclusion of their data in a public directory, of the purpose of that directory and of the fact that those data could be communicated to another telephone service provider and that it is guaranteed that those data will not, once passed on, be used for purposes other than those for which they were collected with a view to their first publication.

ID: f3d4c284-3a6e-48b3-ad0a-2340a5e8085a

Judgment of 2 Mar 2021, C-746/18 (  
Prokuratuur  
)  
Charter of fundamental rights of the EU   
 >   
Article 7 - Respect for private and family life   
Charter of fundamental rights of the EU   
 >   
 Article 8 - Protection of personal data   
Charter of fundamental rights of the EU   
 >   
Article 11 - Freedom of expression and information   
Charter of fundamental rights of the EU   
 >   
Article 52 - Scope of guaranteed rights   
E-privacy Directive   
 >   
Electronic communications   
 >   
Application of certain general data protection provisions   
E-privacy Directive   
 >   
Electronic communications   
 >   
Traffic data   
E-privacy Directive   
 >   
Electronic communications   
 >   
Location data   
   
JUDGMENT OF THE COURT (Grand Chamber)  
2 March 2021 (\*)  
(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Directive 2002/58/EC – Providers of electronic communications services – Confidentiality of the communications – Limitations – Article 15(1) – Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union – Legislation providing for the general and indiscriminate retention of traffic and location data by providers of electronic communications services – Access of national authorities to retained data for the purpose of investigations – Combating of crime in general – Authorisation given by the public prosecutor’s office – Use of data in criminal proceedings as evidence – Admissibility)  
In Case C-746/18,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Riigikohus (Supreme Court, Estonia), made by decision of 12 November 2018, received at the Court on 29 November 2018, in criminal proceedings against  
H. K.,  
other party:  
Prokuratuur,   
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, J.-C. Bonichot, A. Arabadjiev, A. Prechal and L. Bay Larsen, Presidents of Chambers, T. von Danwitz (Rapporteur), M. Safjan, K. Jürimäe, C. Lycourgos and P.G. Xuereb, Judges,  
Advocate General: G. Pitruzzella,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 15 October 2019,  
after considering the observations submitted on behalf of:  
–        H. K., by S. Reinsaar, vandeadvokaat,  
–        the Prokuratuur, by T. Pern and M. Voogma, acting as Agents,  
–        the Estonian Government, by N. Grünberg, acting as Agent,  
–        the Danish Government, by J. Nymann-Lindegren and M.S. Wolff, acting as Agents,  
–        Ireland, by M. Brown, G. Hodge, J. Quaney and A. Joyce, acting as Agents, and D. Fennelly, Barrister-at-Law,  
–        the French Government, initially by D. Dubois, D. Colas, E. de Moustier and A.-L. Desjonquères, and subsequently by D. Dubois, E. de Moustier and A.-L. Desjonquères, acting as Agents,  
–        the Latvian Government, initially by V. Kalniņa and I. Kucina, and subsequently by V. Soņeca and V. Kalniņa, acting as Agents,  
–        the Hungarian Government, by M.Z. Fehér and A. Pokoraczki, acting as Agents,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes, P. Barros da Costa, L. Medeiros and I. Oliveira, acting as Agents,  
–        the Finnish Government, by J. Heliskoski, acting as Agent,  
–        the United Kingdom Government, by S. Brandon and Z. Lavery, acting as Agents, G. Facenna QC and C. Knight, Barrister,  
–        the European Commission, initially by H. Kranenborg, M. Wasmeier, P. Costa de Oliveira and K. Toomus, and subsequently by H. Kranenborg, M. Wasmeier and E. Randvere, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 21 January 2020,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’).  
2        The request has been made in the context of criminal proceedings brought against H. K. on counts of theft, use of another person’s bank card and violence against persons party to court proceedings.  
   
Legal context  
   
EU law  
3        Recitals 2 and 11 of Directive 2002/58 state:  
‘(2)      This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the [Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of [the] Charter.  
…  
(11)      Like Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, [signed in Rome on 4 November 1950,] as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.’  
4        Article 2 of Directive 2002/58, headed ‘Definitions’, provides:  
‘Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.  
The following definitions shall also apply:  
(a)      “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;  
(b)      “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  
(c)      “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;  
(d)      “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;  
…’  
5        As set out in Article 5 of Directive 2002/58, headed ‘Confidentiality of the communications’:  
‘1.      Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.  
…  
3.      Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’  
6        Article 6 of Directive 2002/58, headed ‘Traffic data’, provides:  
‘1.      Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).  
2.      Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.  
3.      For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  
…  
5.      Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.  
…’  
7        Article 9 of Directive 2002/58, headed ‘Location data other than traffic data’, provides in paragraph 1:  
‘Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …’  
8        Article 15 of Directive 2002/58, headed ‘Application of certain provisions of Directive [95/46]’, states in paragraph 1:  
‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of [EU] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’  
   
E  
stoni  
a  
n  
 law  
   
The Law on electronic communications   
9        Paragraph 1111 of the elektroonilise side seadus (Law on electronic communications, RT I 2004, 87, 593; RT I, 22.05.2018, 3), in the version applicable at the material time (‘the Law on electronic communications’), a provision which is headed ‘Obligation to retain data’, states:  
‘…  
(2)      Providers of telephone and mobile telephone services and of telephone network and mobile telephone network services are obliged to retain the following data:  
1)      the number of the calling party and the name and address of the subscriber;  
2)      the number of the called party and the name and address of the subscriber;  
3)      when use is made of an additional service, including call forwarding or call transfer, the number dialled and the name and address of the subscriber;  
4)      the date and time of the start and end of the call;  
5)      the telephone or mobile telephone service used;  
6)      the International Mobile Subscriber Identity (IMSI) of the calling and called party;  
7)      the International Mobile Equipment Identity (IMEI) of the calling and called party;  
8)      the cell ID at the start of the call;  
9)      data on the geographical location of the base station by reference to its cell ID during the period for which data are retained;  
10)      in the case of pre-paid anonymous mobile telephone services, the date and time of the initial activation of the service and the cell ID from which the service was activated.  
…  
(4)      The data referred to in subparagraphs 2 and 3 of this paragraph shall be retained for one year from the time of the communication if those data were generated or processed in the course of providing a communications service. …  
…  
(11)      The data referred to in subparagraphs 2 and 3 of this paragraph shall be forwarded:  
1)      in accordance with the kriminaalmenetluse seadustik (Code of Criminal Procedure), to an investigating authority, a surveillance authority, the public prosecutor’s office and the court;  
…’  
   
The Code of Criminal Procedure  
10      Paragraph 17 of the Code of Criminal Procedure (kriminaalmenetluse seadustik, RT I 2003, 27, 166 ; RT I, 31.05.2018, 22) provides:  
(1)      The parties to court proceedings are the public prosecutor’s office …  
…’  
11      Paragraph 30 of that code is worded as follows:  
‘(1)       The public prosecutor’s office shall direct the pre-trial procedure, guaranteeing its lawfulness and effectiveness, and represent the public prosecution before the court.  
(2)      The powers of the public prosecutor’s office in criminal proceedings shall be exercised in the name of the public prosecutor’s office by a public prosecutor who acts independently and is only bound by the law.’  
12      Paragraph 901 of the code provides:  
‘…  
(2)      The investigating authority may, in the pre-trial procedure with the authorisation of the public prosecutor’s office or in judicial proceedings with the authorisation of the court, ask an electronic communications undertaking for the data listed in Paragraph 1111(2) and (3) of the Law on electronic communications which is not specified in subparagraph 1 of the present paragraph. The authorisation of the request shall note the period for which the data request is allowed with precise date indications.   
(3)      A request may be made pursuant to this paragraph only where this is essential for achieving the objective of the criminal proceedings.’  
13      Paragraph 211 of the code states:  
‘(1)      The objective of the pre-trial procedure is to gather evidence and create the other conditions for judicial proceedings.  
(2)      In the pre-trial procedure, the investigating authority and the public prosecutor’s office shall ascertain the circumstances exonerating and incriminating the suspect or accused.’  
   
The Law on the public prosecutor’s office   
14      Paragraph 1 of the prokuratuuriseadus (Law on the public prosecutor’s office, RT I 1998, 41, 625; RT I, 06.07.2018, 20), in the version applicable at the material time, provides:  
‘(1)      The public prosecutor’s office is a government authority falling under the jurisdiction of the Ministry of Justice which participates in planning the monitoring activities necessary for fighting and investigating criminal offences, directs the pre-trial procedure, guaranteeing its lawfulness and effectiveness, represents the public prosecution before the court, and performs other duties assigned to the prosecutor’s office by law.  
(11)      The public prosecutor’s office shall perform its statutory duties independently and act in accordance with the present law, other laws and legislation adopted on the basis of those laws.  
…’  
15      Paragraph 2(2) of that law states:  
‘The public prosecutor shall perform his or her duties independently and act exclusively according to the law and his or her convictions.’  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
16      By judgment of 6 April 2017, the Viru Maakohus (Court of First Instance, Viru, Estonia) imposed on H. K. a custodial sentence of two years for having committed, between 17 January 2015 and 1 February 2016, a number of thefts of goods (of a value ranging from EUR 3 to EUR 40) and cash (in amounts between EUR 5.20 and EUR 2 100), used another person’s bank card, causing that person a loss of EUR 3 941.82, and performed acts of violence against persons party to court proceedings concerning her.  
17      In order to find H. K. guilty of those acts, the Viru Maakohus (Court of First Instance, Viru) relied, inter alia, on several reports which were drawn up on the basis of data relating to electronic communications, as referred to in Paragraph 1111(2) of the Law on electronic communications, that the investigating authority had obtained in the pre-trial procedure from a provider of electronic telecommunications services, after having been granted several authorisations for that purpose by the Viru Ringkonnaprokuratuur (Viru District Public Prosecutor’s Office, Estonia) in accordance with Paragraph 901 of the Code of Criminal Procedure. Those authorisations, granted on 28 January and 2 February 2015, 2 November 2015 and 25 February 2016, related to data concerning several telephone numbers of H. K. and various IMEI codes of hers, in respect of the period from 1 January to 2 February 2015, of 21 September 2015, and of the period from 1 March 2015 to 19 February 2016.  
18      H. K. brought an appeal against the judgment of the Viru Maakohus (Court of First Instance, Viru) before the Tartu Ringkonnakohus (Court of Appeal, Tartu, Estonia), which dismissed the appeal by judgment of 17 November 2017.  
19      H. K. lodged an appeal on a point of law against the latter judgment before the Riigikohus (Supreme Court, Estonia), contesting, inter alia, the admissibility of the reports drawn up on the basis of the data obtained from the provider of electronic communications services. In her submission, it follows from the judgment of 21 December 2016,   
Tele2 Sverige and Watson and Others  
 (C-203/15 and C-698/15, ‘  
Tele2  
’, EU:C:2016:970), that the provisions of Paragraph 1111 of the Law on electronic communications which lay down the obligation on service providers to retain communications data, as well as the use of such data for the purpose of her conviction, are contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.  
20      According to the referring court, the question arises whether the reports drawn up on the basis of data referred to in Paragraph 1111(2) of the Law on electronic communications may be regarded as constituting admissible evidence. That court observes that the admissibility of the reports at issue in the main proceedings as evidence depends on the question of the extent to which the gathering of the data on the basis of which those reports were drawn up was in conformity with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.  
21      The referring court considers that, in order to answer that question, it needs to be determined whether Article 15(1) of Directive 2002/58, read in the light of the Charter, must be interpreted as meaning that the access of State authorities to data making it possible to identify the source and destination of a telephone communication from a suspect’s landline or mobile telephone, to determine the date, time, duration and type of that communication, to identify the communications equipment used and to establish the location of the mobile communication equipment used amounts to interference with the fundamental rights at issue which is so serious that such access should be restricted to combating serious crime, regardless of the period in respect of which the State authorities have sought access to the retained data.  
22      The referring court takes the view, however, that the length of that period is an essential factor for assessing the seriousness of the interference represented by access to traffic and location data. Thus, where that period is very short or the quantity of data gathered is very limited, the question should be raised whether the objective of combating crime in general, and not only combating serious crime, is capable of justifying such an interference.  
23      Finally, the referring court has doubts as to whether it is possible to regard the Estonian public prosecutor’s office as an independent administrative authority, for the purposes of paragraph 120 of the judgment of 21 December 2016,   
Tele2  
 (C-203/15 and C-698/15, EU:C:2016:970), which is capable of authorising access of the investigating authority to data relating to electronic communications such as the data referred to in Paragraph 1111(2) of the Law on electronic communications.  
24      The referring court states that the public prosecutor’s office directs the pre-trial procedure, while guaranteeing its lawfulness and effectiveness. Since the objective of that procedure is, inter alia, to gather evidence, the investigating authority and the public prosecutor’s office verify the circumstances incriminating and exonerating any suspect or person accused. If the public prosecutor’s office is satisfied that all the necessary evidence has been gathered, it brings the public prosecution against the accused. The powers of the public prosecutor’s office are exercised in its name by a public prosecutor who carries out his or her duties independently, as follows from Paragraph 30(1) and (2) of the Code of Criminal Procedure and Paragraphs 1 and 2 of the Law on the public prosecutor’s office.  
25      In that context, the referring court observes that its doubts as to the independence required by EU law are principally attributable to the fact that the public prosecutor’s office not only directs the pre-trial procedure, but also represents the public prosecution at the trial, that authority being, pursuant to national law, party to the criminal proceedings.  
26      It was in those circumstances that the Riigikohus (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Is Article 15(1) of Directive [2002/58], in conjunction with Articles 7, 8, 11 and 52(1) of the [Charter], to be interpreted as meaning that in criminal proceedings the access of State authorities to data making it possible to establish the source and destination, the date, the time, the duration and the type of the communication, the terminal used and the location of the mobile terminal used, in relation to a telephone or mobile telephone communication of a suspect, constitutes so serious an interference with the fundamental rights enshrined in those articles of the Charter that that access in the area of prevention, investigation, detection and prosecution of criminal offences must be restricted to the fighting of serious crime, regardless of the period to which the retained data to which the State authorities have access relate?  
(2)      Is Article 15(1) of Directive [2002/58], on the basis of the principle of proportionality expressed in the judgment of [2 October 2018,  
 Ministerio Fiscal  
 (C-207/16, EU:C:2018:788)], paragraphs 55 to 57, to be interpreted as meaning that, if the amount of data mentioned in the first question, to which the State authorities have access, is not large (both in terms of the type of data and in terms of its temporal extent), the associated interference with fundamental rights is justified by the objective of prevention, investigation, detection and prosecution of criminal offences generally, and that the greater the amount of data to which the State authorities have access, the more serious the criminal offences which are intended to be fought by the interference must be?  
(3)      Does the requirement mentioned in the judgment of [21 December 2016,   
Tele2  
 (C-203/15 and C-698/15, EU:C:2016:970)], second point of the operative part, that the data access of the competent State authorities must be subject to prior review by a court or an independent administrative authority mean that Article 15(1) of Directive [2002/58] must be interpreted as meaning that the public prosecutor’s office which directs the pre-trial procedure, with it being obliged by law to act independently and only being bound by the law, and ascertains the circumstances both incriminating and exonerating the accused in the pre-trial procedure, but later represents the public prosecution in the judicial proceedings, may be regarded as an independent administrative authority?’  
   
Consideration of the questions referred  
   
The f  
irst and second  
 questions  
27      By its first and second questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime, regardless of the length of the period in respect of which access to those data is sought and the quantity and the nature of the data available in respect of such a period.  
28      It is apparent from the request for a preliminary ruling that, as the Estonian Government confirmed at the hearing, the data to which the national investigating authority had access in the main proceedings is the data kept under Paragraph 1111(2) and (4) of the Law on electronic communications, which obliges providers of electronic communications services to retain, generally and indiscriminately, for one year traffic and location data so far as concerns fixed and mobile telephony. Those data make it possible, in particular, to trace and identify the source and destination of a communication from a person’s landline or mobile telephone, to determine the date, time, duration and type of that communication, to identify the communications equipment used, and to establish the location of the mobile telephone without a communication necessarily being conveyed. In addition, they enable the frequency of a user’s communications with certain persons over a given period of time to be established. Furthermore, as the Estonian Government confirmed at the hearing, access to those data may, in relation to combating crime, be sought in respect of any type of criminal offence.  
29      As regards the circumstances in which access to traffic and location data retained by providers of electronic communications services may, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, be granted to public authorities, pursuant to a measure adopted under Article 15(1) of Directive 2002/58, the Court has held that such access may be granted only in so far as those data have been retained by a provider in a manner that is consistent with Article 15(1) (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 167).  
30      In this connection, the Court has also held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precludes legislative measures which, for such purposes, provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168).  
31      As to the objectives capable of justifying public authorities having access to data retained by providers of electronic communications services pursuant to a measure consistent with those provisions, it is apparent, first, from the Court’s case-law that such access may be justified only by the public interest objective for which those service providers were ordered to retain the data (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 166).  
32      Second, the Court has held that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to the seriousness of the interference (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 131 and the case-law cited).  
33      So far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue in the main proceedings, in accordance with the principle of proportionality only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data, whether the retention be general and indiscriminate or targeted. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective, pursued by the legislation at issue in the main proceedings, of preventing, investigating, detecting and prosecuting criminal offences in general (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 140 and 146).  
34      In that regard, it has inter alia been held that legislative measures concerning the processing of data in themselves relating to the civil identity of users of electronic communications systems, including the retention of and access to those data, solely for the purpose of identifying the user concerned, and without it being possible for those data to be associated with information on the communications made, are capable of being justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general, to which the first sentence of Article 15(1) of Directive 2002/58 refers. Those data do not, in themselves, make it possible to ascertain the date, time, duration and recipients of the communications made, or the locations where those communications took place or their frequency with specific people during a given period, with the result that they do not provide, apart from the contact details of users of means of electronic communication, such as their addresses, any information on the communications sent and, consequently, on the users’ private lives. Thus, the interference entailed by a measure relating to those data cannot, in principle, be classified as serious (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 157 and 158 and the case-law cited).  
35      Accordingly, only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and that allow precise conclusions to be drawn concerning the private lives of the persons concerned (see, to that effect, judgment of 2 October 2018,   
Ministerio Fiscal  
, C-207/16, EU:C:2018:788, paragraph 54), and other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to such data is sought, cannot have the effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access.  
36      Access to a set of traffic or location data, such as the data retained pursuant to Paragraph 1111 of the Law on electronic communications, is indeed liable to allow precise, or even very precise, conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 117).  
37      It is true that, as the referring court suggests, the longer that the period is in respect of which access is sought, the greater, in principle, is the quantity of data liable to be retained by providers of electronic communications services, regarding the electronic communications sent, the places of residence stayed in and the movements made by the user of a means of electronic communication, thus allowing a greater number of conclusions concerning that user’s private life to be drawn from the data consulted. A similar finding may be made so far as concerns the categories of data sought.  
38      It is, therefore, for the purpose of satisfying the requirement of proportionality, under which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130 and the case-law cited), that it is for the competent national authorities to ensure, in each individual case, that both the category or categories of data covered and the period in respect of which access to those data is sought are, on the basis of the circumstances of the case, limited to what is strictly necessary for the purposes of the investigation in question.  
39      However, the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter that is entailed by a public authority’s access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses, is in any event serious regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period, when, as in the main proceedings, that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned.  
40      Even access to a limited quantity of traffic or location data or access to data in respect of a short period may be liable to provide precise information on the private life of a user of a means of electronic communication. Furthermore, the quantity of the data available and the specific information on the private life of the person concerned that results from the data are matters that can be assessed only after the data have been consulted. However, authorisation of access, granted by the court having jurisdiction or the competent independent authority, necessarily occurs before the data and the information resulting therefrom can be consulted. Thus, the assessment of the seriousness of the interference that the access constitutes is necessarily carried out on the basis of the risk generally pertaining to the category of data sought for the private lives of the persons concerned, without it indeed mattering whether or not the resulting information relating to the person’s private life is in actual fact sensitive.  
41      Finally, given the fact that the referring court has before it a claim that the reports drawn up on the basis of the traffic and location data are inadmissible, on the ground that Paragraph 1111 of the Law on electronic communications is contrary to Article 15(1) of Directive 2002/58 as regards both retention of and access to data, it should be noted that, as EU law currently stands, it is, in principle, for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed criminal offences, of information and evidence obtained by general and indiscriminate retention of such data contrary to EU law (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 222) or by access of the national authorities thereto contrary to EU law.  
42      The Court has consistently held that, in the absence of EU rules on the matter, it is for the national legal order of each Member State, in accordance with the principle of procedural autonomy, to establish procedural rules for actions intended to safeguard the rights that individuals derive from EU law, provided, however, that those rules are no less favourable than the rules governing similar situations subject to domestic law (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness) (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 223 and the case-law cited).  
43      As regards the principle of effectiveness in particular, it should be noted that the objective of national rules on the admissibility and use of information and evidence is, in accordance with the choices made by national law, to prevent information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences. That objective may be achieved under national law not only by prohibiting the use of such information and evidence, but also by means of national rules and practices governing the assessment and weighting of such material, or by factoring in whether that material is unlawful when determining the sentence (judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 225).  
44      In deciding whether to exclude information and evidence obtained in contravention of the requirements of EU law, regard must be had, in particular, to the risk of breach of the adversarial principle and, therefore, of the right to a fair trial entailed by the admissibility of such information and evidence. If a court takes the view that a party is not in a position to comment effectively on evidence pertaining to a field of which the judges have no knowledge and that is likely to have a preponderant influence on the findings of fact, it must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an infringement. Therefore, the principle of effectiveness requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law or by means of access of the competent authority thereto in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 226 and 227).  
45      In the light of the foregoing considerations, the answer to the first and second questions is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period.  
   
T  
he t  
hird  
 question  
46      By its third question, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that confers upon the public prosecutor’s office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.  
47      The referring court explains in this connection that, whilst the Estonian public prosecutor’s office is, under national law, obliged to act independently, is subject only to the law and must examine the incriminating and exculpatory evidence in the pre-trial procedure, the objective of that procedure nevertheless remains the gathering of evidence and fulfilment of the other conditions necessary for judicial proceedings. It states that it is that authority which represents the public prosecution at the trial and it is therefore also party to the proceedings. Furthermore, it is apparent from the documents before the Court that, as the Estonian Government and the Prokuratuur also confirmed at the hearing, the Estonian public prosecutor’s office is organised hierarchically and that requests for access to traffic and location data are not subject to particular formal requirements and may be made by the public prosecutor him or herself. Finally, the persons to whose data access may be granted are not only those suspected of involvement in a criminal offence.  
48      It is true that, as the Court has already held, it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to the data in their possession. However, in order to satisfy the requirement of proportionality, such legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary (see, to that effect, judgments of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 117 and 118; of 6 October 2020,   
Privacy International  
, C-623/17, EU:C:2020:790, paragraph 68; and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).  
49      In particular, national legislation governing the access of the competent authorities to retained traffic and location data, adopted pursuant to Article 15(1) of Directive 2002/58, cannot be limited to requiring that the authorities’ access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (judgments of 6 October 2020,   
Privacy International  
, C-623/17, EU:C:2020:790, paragraph 77, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 176 and the case-law cited).  
50      Accordingly, and since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities (see, to that effect, judgments of 21 December 2016,   
Tele2  
, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119, and of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 188).  
51      In order to ensure, in practice, that those conditions are fully observed, it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. In cases of duly justified urgency, the review must take place within a short time (see, to that effect, judgment of 6 October 2020,   
La Quadrature du Net and Others  
, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 189 and the case-law cited).  
52      As the Advocate General has observed, in essence, in point 105 of his Opinion, one of the requirements for that prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access.  
53      Where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence (see, to that effect, judgment of 9 March 2010,   
Commission  
 v   
Germany  
, C-518/07, EU:C:2010:125, paragraph 25, and Opinion 1/15 (  
EU-Canada PNR Agreement  
) of 26 July 2017, EU:C:2017:592, paragraphs 229 and 230).  
54      It follows from the foregoing considerations that the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review referred to in paragraph 51 of the present judgment means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field, as the Advocate General has observed, in essence, in point 126 of his Opinion, the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings.  
55      That is not so in the case of a public prosecutor’s office which directs the investigation procedure and, where appropriate, brings the public prosecution. The public prosecutor’s office has the task not of ruling on a case in complete independence but, acting as prosecutor in the proceedings, of putting it, where appropriate, before the court that has jurisdiction.  
56      The fact that the public prosecutor’s office may, in accordance with the rules governing its powers and status, be required to verify the incriminating and exculpatory evidence, to guarantee the lawfulness of the pre-trial procedure and to act exclusively according to the law and the prosecutor’s convictions cannot be sufficient to confer upon it the status of a third party in relation to the interests at issue as referred to in paragraph 52 of the present judgment.  
57      It follows that the public prosecutor’s office is not in a position to carry out the prior review referred to in paragraph 51 of the present judgment.  
58      Since the referring court has raised, furthermore, the issue whether the lack of a review by an independent authority may be made up for by a subsequent review carried out by a court as to whether a national authority’s access to traffic and location data was lawful, it must be pointed out that, as required by the case-law recalled in paragraph 51 of the present judgment, the independent review must take place before any access, except in the event of duly justified urgency, in which case the review must take place within a short time. As the Advocate General has stated in point 128 of his Opinion, such subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met.  
59      Accordingly, the answer to the third question referred for a preliminary ruling is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that confers upon the public prosecutor’s office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.  
   
Costs  
60      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period.  
2.        
Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation that confers upon the public prosecutor’s office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.

ID: fc55f29e-68c0-46c7-857a-7f3a13dc2ba5

of 5 Dec 2023, C-683/21 (  
Nacionalinis visuomenės sveikatos centras  
)  
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
 Definitions - Data Controller   
General data protection law   
 >   
Chapter IV - Controller and processor   
 >   
Joint controllers   
General data protection law   
 >   
Chapter I - General Provisions   
 >   
Definitions - Processing   
General data protection law   
 >   
Chapter VIII - Remedies, liability and penalties   
 >   
Administrative fines   
   
JUDGMENT OF THE COURT (Grand Chamber)  
5 December 2023 (\*)  
(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 4(2) and (7) – Concepts of ‘processing’ and ‘controller’ – Development of a mobile IT application – Article 26 – Joint control – Article 83 – Imposition of administrative fines – Conditions – Requirement that the infringement be intentional or negligent – Responsibility and liability of the controller for the processing of personal data carried out by a processor)  
In Case C-683/21,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania), made by decision of 22 October 2021, received at the Court on 12 November 2021, in the proceedings  
Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos  
v  
Valstybinė duomenų apsaugos inspekcija,  
interveners:  
UAB ‘IT sprendimai sėkmei’,  
Lietuvos Respublikos sveikatos apsaugos ministerija,  
THE COURT (Grand Chamber),  
composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, C. Lycourgos, E. Regan, T. von Danwitz, Z. Csehi, O. Spineanu-Matei, Presidents of Chambers, M. Ilešič, J.-C. Bonichot, L.S. Rossi, A. Kumin, N. Jääskinen (Rapporteur), N. Wahl and M. Gavalec, Judges,  
Advocate General: N. Emiliou,  
Registrar: C. Strömholm, Administrator,  
having regard to the written procedure and further to the hearing on 17 January 2023,  
after considering the observations submitted on behalf of:  
–        the Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, by G. Aleksienė,  
–        the Valstybinė duomenų apsaugos inspekcija, by R. Andrijauskas,  
–        the Lithuanian Government, by V. Kazlauskaitė-Švenčionienė, acting as Agent,  
–        the Netherlands Government, by C.S. Schillemans, acting as Agent,  
–        the Council of the European Union, by R. Liudvinavičiūtė and K. Pleśniak, acting as Agents,  
–        the European Commission, by A. Bouchagiar, H. Kranenborg and A. Steiblytė, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 4 May 2023,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 4(2) and (7), Article 26(1) and Article 83(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’).  
2        The request has been made in proceedings between the Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (National Public Health Centre under the Ministry of Health, Lithuania; ‘the NVSC’) and the Valstybinė duomenų apsaugos inspekcija (State Data Protection Inspectorate, Lithuania; ‘the VDAI’) concerning a decision by which the VDAI imposed an administrative fine on the NVSC pursuant to Article 83 of the GDPR for infringement of Articles 5, 13, 24, 32 and 35 of that regulation.  
   
Legal context  
   
European Union law  
3        Recitals 9, 10, 11, 13, 26, 74, 79, 129 and 148 of the GDPR state:  
‘(9)      … Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the [European] Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. …  
(10)      In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …  
(11)      Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.  
…  
(13)      In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. …  
…  
(26)      The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information[,] should be considered to be information on an identifiable natural person. … The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.  
…  
(74)      The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.  
…  
(79)      The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors … requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.  
…  
(129)      In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions … The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular[,] each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.  
…  
(148)      In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of[,] appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the [Charter of Fundamental Rights of the European Union], including effective judicial protection and due process.’  
4        According to Article 4 of that regulation:  
‘For the purposes of this Regulation:  
(1)      “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  
(2)      “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  
…  
(5)      “pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;  
…  
(7)      “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;  
(8)      “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;  
…’  
5        Article 26 of the GDPR, entitled ‘Joint controllers’, states, in paragraph 1 thereof:  
‘Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.’  
6        Article 28 of that regulation, entitled ‘Processor’, provides, in paragraph 10 thereof:  
‘Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.’  
7        Article 58 of the GDPR, entitled ‘Powers’, provides, in paragraph 2 thereof:  
‘Each supervisory authority shall have all of the following corrective powers:  
(a)      to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;  
(b)      to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;  
…  
(d)      to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;  
…  
(f)      to impose a temporary or definitive limitation including a ban on processing;  
…  
(i)      to impose an administrative fine pursuant to Article 83, in addition to, or instead of[,] measures referred to in this paragraph, depending on the circumstances of each individual case;  
…’  
8        Article 83 of that regulation, entitled ‘General conditions for imposing administrative fines’, is worded as follows:  
‘1.      Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.  
2.      Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine[,] in each individual case due regard shall be given to the following:  
(a)      the nature, gravity and duration of the infringement taking into account the nature[,] scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;  
(b)      the intentional or negligent character of the infringement;  
(c)      any action taken by the controller or processor to mitigate the damage suffered by data subjects;  
(d)      the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;  
(e)      any relevant previous infringements by the controller or processor;  
(f)      the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;  
(g)      the categories of personal data affected by the infringement;  
(h)      the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;  
(i)      where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject matter, compliance with those measures;  
(j)      adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and  
(k)      any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.  
3.      If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.  
4.      Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to [EUR 10 000 000], or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:  
(a)      the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;  
…  
5.      Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to [EUR 20 000 000], or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:  
(a)      the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;  
(b)      the data subjects’ rights pursuant to Articles 12 to 22;  
…  
(d)      any obligations pursuant to Member State law adopted under Chapter IX;  
…  
6.      Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to [EUR 20 000 000], or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.  
7.      Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.  
8.      The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.  
…’  
9        Article 84 of the GDPR, entitled ‘Penalties’, provides, in paragraph 1 thereof:  
‘Member States shall lay down the rules on other penalties applicable to infringements of this Regulation[,] in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.’  
   
Lithuanian law  
10      Article 29(3) of the Viešųjų pirkimų įstatymas (Law on Public Procurement) refers to certain circumstances in which the contracting authority has the right or the obligation to terminate the procurement or design contest procedures at its own discretion and at any time prior to the award of a public contract (or framework agreement) or to the determination of the successful candidate in a design contest.  
11      Article 72(2) of the Law on Public Procurement lays down the stages of the negotiations which are to be conducted by the contracting authority in the context of a negotiated public procurement procedure without prior publication.  
   
The dispute in the main proceedings and the questions referred for a preliminary ruling  
12      In the context of the pandemic caused by the COVID-19 virus, the Lietuvos Respublikos sveikatos apsaugos ministras (Minister for Health of the Republic of Lithuania), by an initial decision of 24 March 2020, instructed the Director of the NVSC to organise the immediate acquisition of an IT system for the registration and monitoring of the data of persons exposed to that virus, for the purposes of epidemiological follow-up.  
13      By email of 27 March 2020, a person claiming to be a representative of the NVSC (‘A.S.’) informed the company UAB ‘IT sprendimai sėkmei’ (‘the company ITSS’) that the NVSC had selected it to create a mobile application for that purpose. A.S. subsequently sent emails to the company ITSS relating to various aspects of the creation of that application, and a copy of those emails was sent to the Director of the NVSC.  
14      In the course of the negotiations between the company ITSS and the NVSC, in addition to A.S., other employees of the NVSC also sent emails to that company concerning the drafting of the questions asked in the mobile application at issue.  
15      During the creation of that mobile application, a confidentiality policy was drawn up, in which the company ITSS and the NVSC were designated as controllers.  
16      The mobile application at issue, which referred to the company ITSS and the NVSC, was available for download in the online shop Google Play Store as from 4 April 2020 and in the online shop Apple App Store as from 6 April 2020. It was operational until 26 May 2020.  
17      From 4 April 2020 to 26 May 2020, 3 802 persons used that application and provided data relating to them as requested by the application, such as their ID number, geographical coordinates (latitude and longitude), country, city, municipality, postcode, street name, building number, surname, first name, personal identification number, telephone number and address.  
18      By a further decision of 10 April 2020, the Minister for Health of the Republic of Lithuania decided to entrust the Director of the NVSC with the task of organising the acquisition of the mobile application at issue from the company ITSS and, for that purpose, it was envisaged that recourse would be had to Article 72(2) of the Law on Public Procurement. However, no public contract for the official acquisition of that application by the NVSC was awarded to that company.  
19      On 15 May 2020, the NVSC asked the company ITSS not to make any reference whatsoever to the NVSC in the mobile application at issue. Furthermore, by letter of 4 June 2020, the NVSC informed that company that, due to a lack of funding for the acquisition of that application, it had, in accordance with Article 29(3) of the Law on Public Procurement, terminated the procedure relating to such acquisition.  
20      In the context of an investigation relating to the processing of personal data, initiated on 18 May 2020, the VDAI established that personal data had been collected using the mobile application at issue. Moreover, it was found that the users who had chosen that application as a means of monitoring the isolation made mandatory on account of the COVID-19 pandemic had replied to questions involving the processing of personal data. Those data had allegedly been provided in the replies to the questions asked by the abovementioned application and related, inter alia, to the health status of the data subject and to his or her compliance with the conditions of isolation.  
21      By decision of 24 February 2021, the VDAI imposed an administrative fine of EUR 12 000 on the NVSC pursuant to Article 83 of the GDPR, in view of the infringement by the NVSC of Articles 5, 13, 24, 32 and 35 of that regulation. By that decision, an administrative fine of EUR 3 000 was also imposed on the company ITSS as joint controller.  
22      The NVSC has challenged that decision before the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania), which is the referring court, maintaining that it is the company ITSS which must be regarded as the sole controller, within the meaning of Article 4(7) of the GDPR. The company ITSS, for its part, contends that it acted in the capacity of processor, within the meaning of Article 4(8) of the GDPR, on the instruction of the NVSC which, according to that company, is the sole controller.  
23      The referring court notes that the company ITSS created the mobile application at issue and that the NVSC provided that company with advice regarding the content of the questions asked by that application. It observes that there is, however, no public contract between the NVSC and the company ITSS. In addition, it notes that the NVSC neither consented to nor authorised that application being made available through various online shops.  
24      The referring court states that the creation of the mobile application at issue was intended to implement the objective assigned by the NVSC, namely the management of the COVID-19 pandemic through the creation of an IT tool, and that the processing of personal data was envisaged for that purpose. As regards the role of the company ITSS, it notes that it was not envisaged that that company would pursue objectives other than that of receiving remuneration for the IT product created.  
25      The referring court also observes that, during the VDAI investigation, it was established that the Lithuanian company Juvare Lithuania, which manages the IT system for monitoring and controlling transmissible diseases that pose a risk of contagion, had to receive copies of the personal data collected by the mobile application at issue. Furthermore, for the purpose of testing that application, fictitious data were used, with the exception of the telephone numbers of that company’s employees.  
26      In those circumstances, the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:  
‘(1)      Can the concept of “controller” set out in Article 4(7) of the GDPR be interpreted as meaning that a person who is planning to acquire a data collection tool (mobile application) by way of public procurement, irrespective of the fact that a public procurement contract has not been concluded and that the created product (mobile application), for the acquisition of which a public procurement procedure had been used, has not been transferred, is also to be regarded as a controller?  
(2)      Can the concept of “controller” set out in Article 4(7) of the GDPR be interpreted as meaning that a contracting authority which has not acquired the right of ownership of the created IT product and has not taken possession of it, but where the final version of the created application provides links or interfaces to that public entity and/or [where] the confidentiality policy, which was not officially approved or recognised by the public entity in question, specified that public entity itself as a controller, is also to be regarded as a controller?  
(3)      Can the concept of “controller” set out in Article 4(7) of the GDPR be interpreted as meaning that a person who has not performed any actual data processing operations as defined in Article 4(2) of the GDPR and/or has not provided clear permission/consent to the performance of such operations is also to be regarded as a controller? Is the fact that the IT product used for the processing of personal data was created in accordance with the assignment formulated by the contracting authority significant for the interpretation of the concept of “controller”?  
(4)      If the determination of actual data processing operations is relevant for the interpretation of the concept of “controller”, is the definition of “processing” of personal data under Article 4(2) of the GDPR to be interpreted as also covering situations in which copies of personal data have been used for the testing of IT systems in the process for the acquisition of a mobile application?  
(5)      Can joint control of data in accordance with Article 4(7) and Article 26(1) of the GDPR be interpreted exclusively as involving deliberately coordinated actions in respect of the determination of the purpose and means of data processing, or can that concept also be interpreted as meaning that joint control also covers situations in which there is no clear “arrangement” in respect of the purpose and means of data processing and/or actions are not coordinated between the entities? Are the circumstance relating to the stage in the creation of the means of personal data processing (IT application) at which personal data were processed and the purpose of the creation of the application legally significant for the interpretation of the concept of joint control of data? Can an “arrangement” between joint controllers be understood exclusively as a clear and defined establishment of terms governing the joint control of data?  
(6)      Is the provision in Article 83(1) of the GDPR to the effect that “administrative fines … shall … be effective, proportionate and dissuasive” to be interpreted as also covering cases of imposition of liability on the “controller” when, in the process of the creation of an IT product, the developer also performs personal data processing actions, and do the improper personal data processing actions carried out by the processor always give rise automatically to legal liability on the part of the controller? Is that provision to be interpreted as also covering cases of no-fault liability on the part of the controller?’  
   
Consideration of the questions referred  
   
The first, second and third questions  
27      By its first, second and third questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 4(7) of the GDPR is to be interpreted as meaning that an entity which has entrusted an undertaking with the development of a mobile IT application may be regarded as a controller, within the meaning of that provision, although that entity has not itself performed any personal data processing operations, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application.  
28      Article 4(7) of the GDPR defines the concept of ‘controller’ broadly as the natural or legal person, public authority, agency or any other body which, alone or jointly with others, ‘determines the purposes and means of the processing’ of personal data.  
29      The objective of that broad definition consists, in accordance with the objective pursued by the GDPR, in ensuring effective protection of the fundamental rights and freedoms of natural persons and, in particular, in ensuring a high level of protection of the right of every person to the protection of personal data concerning him or her (see, to that effect, judgments of 29 July 2019,   
Fashion ID  
, C-40/17, EU:C:2019:629, paragraph 66, and of 28 April 2022,   
Meta Platforms Ireland  
, C-319/20, EU:C:2022:322, paragraph 73 and the case-law cited).  
30      The Court has already held that any natural or legal person who exerts influence over the processing of such data, for his, her or its own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller in respect of such processing. In that regard, it is not necessary that the purposes and means of processing be determined by the use of written guidelines or instructions from the controller (see, to that effect, judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraphs 67 and 68); nor is it necessary for that controller to have been formally designated as such.  
31      Therefore, in order to establish whether an entity such as the NVSC may be regarded as a controller within the meaning of Article 4(7) of the GDPR, it is necessary to examine whether that entity actually exerted influence, for its own purposes, over the determination of the purposes and means of the processing in question.  
32      In the present case, subject to matters to be determined by the referring court, it is apparent from the file before the Court of Justice that the creation of the mobile application at issue was commissioned by the NVSC and was intended to implement the objective assigned by that entity, namely the management of the COVID-19 pandemic by means of an IT tool for registering and monitoring the data of persons exposed to the COVID-19 virus. For that purpose, the NVSC had envisaged that the personal data of users of the mobile application at issue would be processed. Furthermore, it is apparent from the order for reference that the parameters of that application, such as the questions asked and their wording, were adapted to the needs of the NVSC and that that entity played an active role in their determination.  
33      In those circumstances, it must, in principle, be considered that the NVSC actually participated in the determination of the purposes and means of the processing.  
34      By contrast, the mere fact that the NVSC was referred to as a controller in the confidentiality policy of the mobile application at issue and that links to that entity were included in that application could be regarded as relevant only if it were established that the NVSC consented, either expressly or implicitly, to such reference or links.  
35      Moreover, the circumstances stated by the referring court in the considerations provided in support of its first three questions referred for a preliminary ruling – namely that the NVSC did not itself process any personal data, that there was no contract between the NVSC and the company ITSS, that the NVSC did not acquire the mobile application at issue and that the dissemination of that application through online shops was not authorised by the NVSC – do not preclude the NVSC from being classified as a ‘controller’ within the meaning of Article 4(7) of the GDPR.  
36      Indeed, it is apparent from that provision, read in the light of recital 74 of the GDPR, that an entity, provided that it satisfies the condition laid down by Article 4(7) of that regulation, is responsible and liable not only for any processing of personal data which it itself carries out, but also for any such processing carried out on its behalf.  
37      In that respect, however, it must be stated that the NVSC cannot be regarded as the controller of personal data processing resulting from the mobile application at issue being made available to the public if, prior to that application being made available, the NVSC expressly objected to such making available, which is a matter for the referring court to ascertain. In such a situation, it cannot be considered that the processing in question was carried out on behalf of the NVSC.  
38      In the light of the foregoing, the answer to the first, second and third questions is that Article 4(7) of the GDPR must be interpreted as meaning that an entity which has entrusted an undertaking with the development of a mobile IT application and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application may be regarded as a controller, within the meaning of that provision, even if that entity has not itself performed any processing operations in respect of such data, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application, unless, prior to that application being made available to the public, that entity expressly objected to such making available and to the resulting processing of personal data.  
   
The fifth question  
39      By its fifth question, which it is appropriate to examine in the second place, the referring court asks, in essence, whether Article 4(7) and Article 26(1) of the GDPR are to be interpreted as meaning that the classification of two entities as joint controllers requires that there be an arrangement between those entities regarding the determination of the purposes and means of the processing of personal data in question or that there be an arrangement laying down the terms of the joint control.  
40      Under Article 26(1) of the GDPR, ‘joint controllers’ exist where two or more controllers jointly determine the purposes and means of processing.  
41      As the Court has held, in order to be regarded as a joint controller, a natural or legal person therefore must independently meet the definition of ‘controller’ laid down in Article 4(7) of the GDPR (see, to that effect, judgment of 29 July 2019,   
Fashion ID  
, C-40/17, EU:C:2019:629, paragraph 74).  
42      However, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case (judgment of 5 June 2018,   
Wirtschaftsakademie Schleswig-Holstein  
, C-210/16, EU:C:2018:388, paragraph 43). Furthermore, the joint responsibility of several actors for the same processing does not require each of them to have access to the personal data concerned (judgment of 10 July 2018,   
Jehovan todistajat  
, C-25/17, EU:C:2018:551, paragraph 69 and the case-law cited).  
43      As the Advocate General observed in point 38 of his Opinion, participation in the determination of the purposes and means of processing can take different forms, since such participation can result from a common decision taken by two or more entities or from converging decisions of those entities. However, where the latter is the case, those decisions must complement each other in such a manner that they each have a tangible impact on the determination of the purposes and means of the processing.  
44      By contrast, it cannot be required that there be a formal arrangement between those controllers as regards the purposes and means of processing.  
45      It is true that, by virtue of Article 26(1) of the GDPR, read in the light of recital 79 of that regulation, joint controllers must, by means of an arrangement between them, determine in a transparent manner their respective responsibilities for compliance with the obligations under that regulation. However, the existence of such an arrangement constitutes not a precondition for two or more entities to be classified as joint controllers, but rather an obligation which Article 26(1) of the GDPR imposes on joint controllers, once they have been classified as such, for the purposes of compliance with their obligations under that regulation. Thus, such classification arises solely from the fact that several entities have participated in the determination of the purposes and means of processing.  
46      In the light of the foregoing, the answer to the fifth question is that Article 4(7) and Article 26(1) of the GDPR must be interpreted as meaning that the classification of two entities as joint controllers does not require that there be an arrangement between those entities regarding the determination of the purposes and means of the processing of personal data in question; nor does it require that there be an arrangement laying down the terms of the joint control.  
   
The fourth question  
47      By its fourth question, the referring court asks, in essence, whether Article 4(2) of the GDPR is to be interpreted as meaning that the use of personal data for the purposes of the IT testing of a mobile application constitutes ‘processing’ within the meaning of that provision.  
48      In the present case, as is apparent from paragraph 25 of the present judgment, the Lithuanian company which manages the IT system for monitoring and controlling transmissible diseases that pose a risk of contagion had to receive copies of the personal data collected by the mobile application at issue. For IT testing purposes, fictitious data were used, with the exception of the telephone numbers of that company’s employees.  
49      In that regard, in the first place, Article 4(2) of the GDPR defines the concept of ‘processing’ as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means’. In a non-exhaustive list, beginning with the wording ‘such as’, that provision refers to the collection, making available and use of personal data as examples of processing.  
50      It is therefore apparent from the wording of that provision, and in particular from the expression ‘any operation’, that the EU legislature intended to confer a broad scope upon the concept of ‘processing’ (see, to that effect, judgment of 24 February 2022,   
Valsts ieņēmumu dienests (Processing of personal data for tax purposes)  
, C-175/20, EU:C:2022:124, paragraph 35), and that the reasons for which an operation or set of operations is performed cannot be taken into account for the purpose of determining whether that operation or set of operations constitutes ‘processing’ within the meaning of Article 4(2) of the GDPR.  
51      Consequently, the question whether personal data are used for the purposes of IT testing or for another purpose has no bearing on whether the operation in question is classified as ‘processing’ within the meaning of that provision.  
52      In the second place, however, it should be pointed out that only processing which relates to ‘personal data’ constitutes ‘processing’ within the meaning of Article 4(2) of the GDPR.  
53      In that regard, Article 4(1) of that regulation states that ‘personal data’ must be understood as meaning ‘any information relating to an identified or identifiable natural person’, that is to say, relating to a ‘natural person … who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.  
54      The fact, alluded to by the referring court in its fourth question, that ‘copies of personal data’ are involved does not, in itself, preclude such copies from being classified as personal data within the meaning of Article 4(1) of the GDPR, provided that those copies actually contain information relating to an identified or identifiable natural person.  
55      However, it must be stated that fictitious data, where they relate not to an identified or identifiable natural person but rather to a person who does not actually exist, do not constitute personal data within the meaning of Article 4(1) of the GDPR.  
56      The same applies with regard to data used for the purposes of IT testing which are anonymous or have been rendered anonymous.  
57      It follows from recital 26 of the GDPR and from the very definition of the concept of ‘personal data’ provided in Article 4(1) of that regulation that neither ‘anonymous information, namely information which does not relate to an identified or identifiable natural person’, nor ‘personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable’, is covered by that concept.  
58      By contrast, it follows from Article 4(5) of the GDPR, read in conjunction with recital 26 of that regulation, that personal data which have undergone only pseudonymisation and which could be attributed to a natural person by the use of additional information must be considered to be information on an identifiable natural person, to which the principles of data protection apply.  
59      In the light of the foregoing, the answer to the fourth question is that Article 4(2) of the GDPR must be interpreted as meaning that the use of personal data for the purposes of the IT testing of a mobile application constitutes ‘processing’, within the meaning of that provision, unless such data have been rendered anonymous in such a manner that the subject of those data is not or is no longer identifiable, or unless it involves fictitious data which do not relate to an existing natural person.  
   
The sixth question  
60      By its sixth question, the referring court asks, in essence, whether Article 83 of the GDPR is to be interpreted as meaning that (i) an administrative fine may be imposed pursuant to that provision only where it is established that the controller has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that article, and (ii) such a fine may be imposed on a controller in respect of processing operations performed by a processor on behalf of that controller.  
61      As regards, in the first place, the question whether an administrative fine may be imposed pursuant to Article 83 of the GDPR only in so far as it is established that the controller or processor has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that article, it is apparent from paragraph 1 thereof that such fines must be effective, proportionate and dissuasive. On the other hand, Article 83 of the GDPR does not expressly state that such an infringement may not be penalised by means of such a fine unless it was committed intentionally or, at the very least, negligently.  
62      The Lithuanian Government and the Council of the European Union infer from this that the EU legislature intended to leave the Member States a certain margin of discretion in the implementation of Article 83 of the GDPR, allowing them to provide for the imposition of administrative fines pursuant to that provision, if necessary, without it being established that the infringement of the GDPR penalised by means of such a fine was committed intentionally or negligently.  
63      Such an interpretation of Article 83 of the GDPR cannot be adopted.  
64      In that regard, it should be recalled that, pursuant to Article 288 TFEU, the provisions of regulations generally have immediate effect in the national legal systems without it being necessary for the national authorities to adopt measures of application. Nonetheless, some provisions of regulations may necessitate, for their implementation, the adoption of measures of application by the Member States (see, to that effect, judgment of 28 April 2022,   
Meta Platforms Ireland  
, C-319/20, EU:C:2022:322, paragraph 58 and the case-law cited).  
65      That is particularly the case for the GDPR, certain provisions of which make it possible for Member States to lay down additional, stricter or derogating national rules, which leave them a margin of discretion as to the manner in which those provisions may be implemented (judgment of 28 April 2022,   
Meta Platforms Ireland  
, C-319/20, EU:C:2022:322, paragraph 57).  
66      Similarly, in the absence of specific procedural rules in the GDPR, it is for the legal system of each Member State, subject to compliance with the principles of equivalence and effectiveness, to prescribe the detailed rules governing actions for safeguarding rights which individuals derive from the provisions of that regulation (see, to that effect, judgment of 4 May 2023,   
Österreichische Post (Non-material damage in connection with the processing of personal data)  
, C-300/21, EU:C:2023:370, paragraphs 53 and 54 and the case-law cited).  
67      However, there is nothing in the wording of Article 83(1) to (6) of the GDPR to suggest that the EU legislature intended to leave the Member States a margin of discretion as regards the substantive conditions which must be satisfied by a supervisory authority where that authority decides to impose an administrative fine on a controller in respect of an infringement referred to in Article 83(4) to (6) of that regulation.  
68      It is true that Article 83(7) of the GDPR provides that each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. Moreover, it is clear from Article 83(8) of that regulation, read in the light of recital 129 thereof, that the exercise by the supervisory authority of its powers under that article is to be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.  
69      However, the fact that the GDPR thereby grants Member States the possibility to lay down exceptions in relation to public authorities and bodies established in those Member States and requirements concerning the procedure to be followed by supervisory authorities in order to impose an administrative fine in no way means that those States are also authorised to lay down, in addition to such exceptions and procedural requirements, substantive conditions which must be satisfied in order to render the controller liable and impose an administrative fine on it pursuant to Article 83 of that regulation. In addition, the fact that the EU legislature took care to make express provision for that possibility but not the possibility to lay down such substantive conditions confirms that it did not leave the Member States a margin of discretion in that regard.  
70      That conclusion is also borne out by a combined reading of Articles 83 and 84 of the GDPR. Article 84(1) of that regulation recognises that Member States retain the power to lay down the rules on ‘other penalties applicable’ to infringements of that regulation, ‘in particular for infringements which are not subject to administrative fines pursuant to Article 83’. It thus follows from such a combined reading of those provisions that the determination of substantive conditions for imposing such administrative fines falls outside the scope of that power. Consequently, such conditions are governed solely by EU law.  
71      As regards the abovementioned conditions, it should be noted that Article 83(2) of the GDPR lists the factors in the light of which the supervisory authority may impose an administrative fine on the controller. Those factors include, in point (b) of that provision, ‘the intentional or negligent character of the infringement’. By contrast, none of the factors listed in the abovementioned provision refers to any possibility of rendering the controller liable in the absence of wrongful conduct on its part.  
72      Furthermore, paragraph 2 of Article 83 of the GDPR must be read in conjunction with paragraph 3 of that article, the purpose of which is to provide for consequences in cases involving multiple infringements of that regulation and according to which ‘if a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement’.  
73      It thus follows from the wording of Article 83(2) of the GDPR that only infringements of the provisions of that regulation which are committed wrongfully by the controller, that is to say, those committed intentionally or negligently, may result in an administrative fine being imposed on that controller pursuant to that article.  
74      The general scheme and purpose of the GDPR support such a reading.  
75      First, the EU legislature provided for a system of sanctions allowing supervisory authorities to impose the most appropriate penalties depending on the circumstances of each individual case.  
76      Article 58 of the GDPR, which determines the powers of supervisory authorities, provides, in paragraph 2(i) thereof, that those authorities may impose administrative fines pursuant to Article 83 of that regulation, ‘in addition to, or instead of’, the other corrective measures listed in Article 58(2) of the GDPR, such as warnings, reprimands or orders. Similarly, recital 148 of that regulation states, inter alia, that, in a case of a minor infringement or if the administrative fine likely to be imposed would constitute a disproportionate burden to a natural person, supervisory authorities may refrain from imposing an administrative fine and instead issue a reprimand.  
77      Second, it is apparent, in particular, from recital 10 of the GDPR that the objectives of the provisions of that regulation are, inter alia, to ensure a consistent and high level of protection of natural persons with regard to the processing of personal data within the Union and, to that end, to ensure consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of such data throughout the Union. In addition, recitals 11 and 129 of the GDPR emphasise the need to ensure, for the purpose of guaranteeing the consistent application of that regulation, that the supervisory authorities have equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and that they can impose equivalent sanctions in the event of infringements of that regulation.  
78      The existence of a system of sanctions, which allows an administrative fine to be imposed pursuant to Article 83 of the GDPR where justified by the specific circumstances of each individual case, provides an incentive for controllers and processors to comply with that regulation. Through their dissuasive effect, administrative fines contribute to strengthening the protection of natural persons with regard to the processing of personal data and are therefore a key element in ensuring respect for the rights of those persons, in accordance with the purpose of that regulation, which is to ensure a high level of protection for such persons with regard to the processing of personal data.  
79      However, the EU legislature did not deem it necessary, for the purpose of ensuring such a high level of protection, to provide for the imposition of administrative fines in the absence of fault. Having regard to the fact that the GDPR aims to achieve a level of protection which is both equivalent and homogenous, and that, to that end, it must be applied consistently throughout the Union, it would be contrary to that purpose to allow the Member States to lay down such a regime for imposing a fine pursuant to Article 83 of that regulation. Moreover, such freedom of choice would be liable to distort competition between economic operators within the Union, which would run counter to the objectives set out by the EU legislature in, inter alia, recitals 9 and 13 of that regulation.  
80      Therefore, it must be found that Article 83 of the GDPR does not allow an administrative fine to be imposed in respect of an infringement referred to in paragraphs 4 to 6 of that article without it being established that such an infringement was committed intentionally or negligently by the controller, and that, accordingly, a wrongful infringement constitutes a condition for imposing such a fine.  
81      In that regard, it must also be stated, in relation to the question whether an infringement has been committed intentionally or negligently and is therefore liable to be penalised by way of an administrative fine under Article 83 of the GDPR, that a controller may be penalised for conduct falling within the scope of the GDPR where that controller could not have been unaware of the infringing nature of its conduct, whether or not it was aware that it was infringing the provisions of the GDPR (see, by analogy, judgments of 18 June 2013,   
Schenker & Co. and Others  
, C-681/11, EU:C:2013:404, paragraph 37 and the case-law cited; of 25 March 2021,   
Lundbeck   
v  
 Commission  
, C-591/16 P, EU:C:2021:243, paragraph 156; and of 25 March 2021,   
Arrow Group and Arrow Generics   
v  
 Commission  
, C-601/16 P, EU:C:2021:244, paragraph 97).  
82      Where the controller is a legal person, it must also be stated that, for Article 83 of the GDPR to apply, it is not necessary for there to have been action by, or even knowledge on the part of, the management body of that legal person (see, by analogy, judgments of 7 June 1983,   
Musique diffusion française and Others   
v  
 Commission  
, 100/80 to 103/80, EU:C:1983:158, paragraph 97, and of 16 February 2017,   
Tudapetrol Mineralölerzeugnisse Nils Hansen   
v  
 Commission  
, C-94/15 P, EU:C:2017:124, paragraph 28 and the case-law cited).  
83      As regards, in the second place, the question whether an administrative fine may be imposed pursuant to Article 83 of the GDPR on a controller in respect of processing operations performed by a processor, it should be recalled that, according to the definition contained in Article 4(8) of that regulation, a processor is ‘a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller’.  
84      Since, as has been stated in paragraph 36 of the present judgment, a controller is responsible and liable not only for any processing of personal data which it itself carries out, but also for any such processing carried out on its behalf, that controller may have an administrative fine imposed on it pursuant to Article 83 of the GDPR in a situation where personal data are unlawfully processed and where it was not such a controller, but rather a processor used by that controller, which carried out the abovementioned processing on behalf of that controller.  
85      However, the responsibility and liability of the controller for the conduct of a processor cannot extend to situations where the processor has processed personal data for its own purposes or where that processor has processed such data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing. In accordance with Article 28(10) of the GDPR, the processor must, in such a situation, be considered to be a controller in respect of such processing.  
86      In the light of the foregoing considerations, the answer to the sixth question is that Article 83 of the GDPR must be interpreted as meaning that (i) an administrative fine may be imposed pursuant to that provision only where it is established that the controller has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that article, and (ii) such a fine may be imposed on a controller in respect of personal data processing operations performed by a processor on behalf of that controller, unless, in the context of those operations, that processor has carried out processing for its own purposes or has processed such data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing.  
   
Costs  
87      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (Grand Chamber) hereby rules:  
1.        
Article 4(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),  
must be interpreted as meaning that an entity which has entrusted an undertaking with the development of a mobile IT application and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application may be regarded as a controller, within the meaning of that provision, even if that entity has not itself performed any processing operations in respect of such data, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application, unless, prior to that application being made available to the public, that entity expressly objected to such making available and to the resulting processing of personal data.  
2.        
Article 4(7) and Article 26(1) of Regulation 2016/679  
must be interpreted as meaning that the classification of two entities as joint controllers does not require that there be an arrangement between those entities regarding the determination of the purposes and means of the processing of personal data in question; nor does it require that there be an arrangement laying down the terms of the joint control.  
3.        
Article 4(2) of Regulation 2016/679  
must be interpreted as meaning that the use of personal data for the purposes of the IT testing of a mobile application constitutes ‘processing’, within the meaning of that provision, unless such data have been rendered anonymous in such a manner that the subject of those data is not or is no longer identifiable, or unless it involves fictitious data which do not relate to an existing natural person.  
4.        
Article 83 of Regulation 2016/679  
must be interpreted as meaning that (i) an administrative fine may be imposed pursuant to that provision only where it is established that the controller has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that article, and (ii) such a fine may be imposed on a controller in respect of personal data processing operations performed by a processor on behalf of that controller, unless, in the context of those operations, that processor has carried out processing for its own purposes or has processed such data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing.

ID: fdf59bf4-6fcd-4fa9-8c8f-88f857c6c052

of 24 Mar 2022, C-245/20 (  
Autoriteit Persoonsgegevens  
)  
General data protection law   
 >   
Chapter VI - Independent supervisory authorities   
 >   
Competence   
   
JUDGMENT OF THE COURT (First Chamber)  
24 March 2022 (\*)  
(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Competence of the supervisory authority – Article 55(3) – Processing operations of courts acting in their judicial capacity – Concept – Making available to a journalist of documents arising from court proceedings containing personal data)  
In Case C-245/20,  
REQUEST for a preliminary ruling under Article 267 TFEU from the Rechtbank Midden-Nederland (District Court, Central Netherlands), made by decision of 29 May 2020, received at the Court on the same day, in the proceedings  
X,  
Z  
v  
Autoriteit Persoonsgegevens  
THE COURT (First Chamber),  
composed of K. Lenaerts, President of the Court, acting as President of the First Chamber, L. Bay Larsen, Vice-President of the Court, N. Jääskinen, J.-C. Bonichot (Rapporteur) and M. Safjan, Judges,  
Advocate General: M. Bobek,  
Registrar: L. Carrasco Marco, Administrator,  
having regard to the written procedure and further to the hearing on 14 July 2021,  
after considering the observations submitted on behalf of:  
–        X and Z, by S.A.J.T. Hoogendoorn, advocaat,  
–        the Autoriteit Persoonsgegevens, by G. Dictus and N.N. Bontje, advocaten,  
–        the Netherlands Government, by K. Bulterman and C.S. Schillemans, acting as Agents,  
–        the Spanish Government, by L. Aguilera Ruiz, acting as Agent,  
–        the Polish Government, by B. Majczyna, acting as Agent,  
–        the Portuguese Government, by L. Inez Fernandes and by P. Barros da Costa, L. Medeiros and I. Oliveira, acting as Agents,  
–        the Finnish Government, by H. Leppo, acting as Agent,  
–        the European Commission, by F. Erlbacher, H. Kranenborg and D. Nardi, acting as Agents,  
after hearing the Opinion of the Advocate General at the sitting on 6 October 2021,  
gives the following  
Judgment  
1        This request for a preliminary ruling concerns the interpretation of Article 55(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).  
2        The request has been made in proceedings between X and Z and the Autoriteit Persoonsgegevens (Data Protection Authority, Netherlands; ‘the AP’) concerning the access of journalists to personal data concerning them, included in a court file, at the hearing held before the Administrative Jurisdiction Division of the Raad van State (Council of State, Netherlands), in proceedings in which Z was a party and represented by X.  
   
Legal context  
   
European Union law   
3        Recital 20 of Regulation 2016/679 states:  
‘While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.’  
4        Under Article 2 of that regulation:  
‘1.      This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.  
2.      This Regulation does not apply to the processing of personal data:  
(a)      in the course of an activity which falls outside the scope of Union law;  
(b)      by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;  
(c)      by a natural person in the course of a purely personal or household activity;  
(d)      by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.  
3.      For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 [of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1)] applies. Regulation [No 45/2001] and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.  
…’  
5        Article 4(2) of the said regulation defines the concept of ‘processing’ as:  
‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’.  
6        Pursuant to Article 51(1) of the same regulation:  
‘Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (“supervisory authority”).’  
7        Last, Article 55 of Regulation 2016/679 provides as follows:  
‘1.      Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.  
2.      Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.  
3.      Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.’  
   
Netherlands law  
8        For the purposes of implementing Regulation 2016/679, the Kingdom of the Netherlands adopted the wet houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) (Law laying down the rules for the implementation of Regulation 2016/679 (Law implementing the General Data Protection Regulation)) of 16 May 2018 (Stb. 2018, No 144). Article 6 of that law entrusts the AP with the task of supervising compliance with Regulation 2016/679 in the Netherlands. None of the provisions of that law reproduces the exception provided for in Article 55(3) of Regulation 2016/679.  
9        On 31 May 2018, the president of the Administrative Jurisdiction Division of the Raad van State (Council of State), the judicial administrations of the Centrale Raad van Beroep (Netherlands) and the College van Beroep voor het bedrijfsleven (Administrative Court of Appeal for Trade and Industry, Netherlands) adopted the regeling verwerking Persoonsgegevens bestuursrechtelijke colleges (Regulation on the processing of personal data in administrative courts). The latter act created the AVG-commissie bestuursrechtelijke colleges (Data Protection Commission for Administrative Law Tribunals, Netherlands; ‘the GDPR Commission’). The latter is responsible for advising the president of the Administrative Jurisdiction Division of the Raad van State (Council of State), the judicial authorities of the Centrale Raad van Beroep (Higher Social Security and Civil Service Court) and the College van Beroep voor het bedrijfsleven (Administrative Court of Appeal for Trade and Industry) on the handling of complaints relating to respect of the rights guaranteed by Regulation 2016/679.  
   
The dispute in the main proceedings and the question referred for a preliminary ruling  
10      At the hearing held on 30 October 2018 before the Administrative Jurisdiction Division of the Raad van State (Council of State) in court proceedings in which Z was a party, represented by X, those two persons were approached by a journalist. During their conversation, X noted that that journalist had at his disposal documents from the case file concerned – including documents that he himself had drafted – showing his name and address in particular as well as Z’s national identification number. That journalist told him that those documents had been made available to him under the right of access to the case file which the Administrative Jurisdiction Division of the Raad van State (Council of State) grants to journalists.  
11      By letter of 21 November 2018, the president of the Administrative Jurisdiction Division of the Raad van State (Council of State) confirmed to X that that division was providing the media with a certain number of documents on pending cases. He informed him that, on the day of the hearing, the communication department of the Raad van State (Council of State) made available to the journalists present documents intended to enable them to follow hearings, namely a copy of the notice of appeal, a copy of the response and, where appropriate, a copy of the contested judicial decision, those documents being destroyed at the end of the day.  
12      X and Z then requested the AP to adopt with regard to the Raad van State (Council of State) ‘enforcement measures’ in respect of the rules on the protection of personal data. By their requests – which were akin to complaints – they claimed that, by allowing journalists to have access to personal data concerning them, originating from the documents in a court file, the Raad van State (Council of State) had infringed Regulation 2016/679.  
13      In response to those requests, the AP stated that, pursuant to Article 55(3) of Regulation 2016/679, it was not competent to supervise processing operations of the personal data concerned, carried out by the Raad van State (Council of State). It subsequently forwarded the requests of X and Z to the GDPR Commission, which in turn forwarded them to the president of the Administrative Jurisdiction Division of the Raad van State (Council of State).  
14      The president of the Administrative Jurisdiction Division of the Raad van State (Council of State) assessed the requests of X and Z as complaints relating to his letter of 21 November 2018 and, after having consulted the GDPR Commission, formulated a new policy on access to documents from court files, which was published on the website of the Raad van State (Council of State).  
15      X and Z challenged, before the referring court, the Rechtbank Midden-Nederland (District Court, Central Netherlands), the decision by which the AP had found itself not competent to hear their requests.  
16      According to that court, giving a journalist access to the documents in a court file containing personal data and making them temporarily available to him or her constitutes ‘processing’ of personal data within the meaning of Article 4(2) of Regulation 2016/679, to which, in this case, X and Z had not consented. With a view to determining whether the AP was indeed not competent to rule on the requests of X and Z, the referring court questions, however, the interpretation that should be given to Article 55(3) of that regulation, which provides that the supervisory authority is not competent to supervise processing operations of courts ‘acting in their judicial capacity’.  
17      It is against this background that the Rechtbank Midden-Nederland (District Court, Central Netherlands) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:  
‘Is Article 55(3) of [Regulation 2016/679] to be interpreted as meaning that “processing operations of courts acting in their judicial capacity” can be understood to mean the provision by a judicial authority of access to procedural documents containing personal data, where such access is granted by making copies of those procedural documents available to a journalist, as described in the order for reference?  
–        In answering that question, is it relevant whether the national supervisory authority’s supervision of that form of data processing affects independent judicial decisions in specific cases?  
–        In answering that question, is it relevant that, according to the judicial authority, the nature and purpose of the data processing is to inform a journalist in order to enable the journalist to better report on a public hearing in court proceedings, thereby serving the interests of openness and transparency in the administration of justice?  
–        In answering that question, is it relevant whether there is any express legal basis for such data processing under national law?’  
   
Consideration of the question referred  
18      By its question, the referring court asks, in essence, whether Article 55(3) of Regulation 2016/679 must be interpreted as meaning that the fact that a court makes temporarily available to journalists documents from court proceedings containing personal data falls within the exercise, by that court, of its ‘judicial capacity’, within the meaning of that provision. In that context, it asks whether, in order to answer that question, it is necessary to take into account the interference which the supervisory authority’s exercise of its powers might have with the independence of the judges in the judgment of specific cases. It also asks whether it is necessary to take into consideration the nature and purpose of that making available of procedural documents – to enable journalists better to report on the course of court proceedings – or indeed whether that making available has an explicit legal basis in domestic law.  
19      As a preliminary point, Z submits, first, that the question referred is hypothetical and that it is, as such, inadmissible. In his view, contrary to what the request for a preliminary ruling indicates, the processing of the data concerned is a matter not for the Administrative Jurisdiction Division of the Raad van State (Council of State), but for the latter’s communication department, which is not a court or tribunal. The request is also vitiated by several other errors or inaccuracies, in particular as regards the status of the person who approached X and Z at the end of the hearing and the exact content of the requests forwarded by the AP to the president of the Administrative Jurisdiction Division of the Raad van State (Council of State).  
20      In that regard, it should be recalled that, according to settled case-law, questions relating to EU law enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court for a preliminary ruling only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the Court does not have before it the legal or factual material necessary to give a useful answer to the questions submitted to it or where the problem is hypothetical (see judgment of 24 November 2020,   
Openbaar Ministerie (Forgery of documents)  
, C-510/19, EU:C:2020:953, paragraph 26 and the case-law cited).  
21      What is more, in proceedings under Article 267 TFEU, which are based on a clear separation of functions between the national courts and the Court, the national court alone has jurisdiction to find and assess the facts in the case before it (see judgment of 26 April 2017,   
Farkas  
, C-564/15, EU:C:2017:302, paragraph 37 and the case-law cited).  
22      It is apparent from the request for a preliminary ruling that the referring court is bound to take a position on the application of Article 55(3) of Regulation 2016/679 to the making available of procedural documents containing personal data at issue in the dispute in the main proceedings to determine whether or not the review of the lawfulness of the latter fell within the AP’s competence. It follows moreover from the case-law cited in the preceding paragraph of the present judgment that Z cannot rebut the presumption enjoyed by the question asked by the referring court merely by disputing the facts it mentions in its request, on which it is not for the Court to take a position. It follows that the plea of inadmissibility raised by Z must be rejected.  
23      Second, Z submits that Article 55(3) of Regulation 2016/679 should be declared invalid by the Court on the ground that the lack of competence of the supervisory authority concerned as regards processing operations carried out by courts ‘acting in their judicial capacity’, provided for by that provision, is not coupled with the obligation for the Member States to lay down specific supervisory arrangements in respect of those processing operations, which he argues is contrary to the requirements arising from the right to an effective remedy.  
24      However, such a line of argument cannot succeed since, as is apparent from recital 20 of Regulation 2016/679, the EU legislature, in enacting Article 55(3) of that regulation, did not intend to shield from all supervision processing operations carried out by courts ‘acting in their judicial capacity’, but merely ruled out the entrusting of the supervision of those operations to an external authority.  
25      In order to answer the question asked by the national court, summarised in paragraph 18 above, it must first of all be noted that Article 2(1) of Regulation 2016/679 provides that that regulation applies to any ‘processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system’, without any distinction being made according to the identity of the person who carried out the processing concerned. It follows that, subject to the cases mentioned in Article 2(2) and (3) thereof, Regulation 2016/679 applies to processing operations carried out both by private persons and by public authorities, including, as recital 20 thereof indicates, judicial authorities, such as courts.  
26      That reading is supported by the fact that several of the provisions of Regulation 2016/679 are subject to adjustments to take account of the specificities of the processing operations carried out by courts. That is particularly the case with Article 55(3) of that regulation, which excludes any competence of the supervisory authority in respect of processing operations carried out by courts ‘acting in their judicial capacity’.  
27      Regulation 2016/679 can be distinguished in that regard from Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC (OJ 2003 L 41, p. 26), which does not apply to courts and tribunals (judgment of 15 April 2021,   
Friends of the Irish Environment  
, C-470/19, EU:C:2021:271  
,   
paragraphs 34  
 to 40  
).  
28      In order to determine the scope of the concept of processing operations carried out by courts acting in their judicial capacity, within the meaning of Article 55(3) of Regulation 2016/679, it must be recalled that the interpretation of a provision of EU law must consider not only its wording, but also the context in which it occurs and the objectives pursued by the legislation of which it is part (see, to that effect, inter alia, judgment of 6 October 2020,   
Jobcenter Krefeld  
, C-181/19, EU:C:2020:794, paragraph 61 and the case-law cited).  
29      In that regard, it is apparent from Article 55 of Regulation 2016/679 that the purpose of that article is to define competence in matters of supervision of the processing of personal data and, in particular, to delimit the competence vested in the national supervisory authority.  
30      Article 55(3) of Regulation 2016/679 thus provides that processing operations carried out by courts ‘acting in their judicial capacity’ fall outside the competence of that supervisory authority.  
31      Recital 20 of Regulation 2016/679, in the light of which that Article 55(3) must be read, states that it should be possible to entrust supervision of processing operations carried out by the courts ‘acting in their judicial capacity’ to specific bodies within the judicial system of the Member State concerned rather than to the supervisory authority under the authority of that Member State, in order to ‘safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making’.  
32      As the Advocate General observed in points 80 and 81 of his Opinion, it is apparent from the very wording of recital 20 of Regulation 2016/679, and in particular from the use of the expression ‘including’, that the scope of the objective pursued by Article 55(3) of that regulation, consisting in safeguarding the independence of the judiciary in the performance of its judicial tasks, cannot be confined solely to guaranteeing the independence of the judges in the adoption of a given judicial decision.  
33      After all, safeguarding the independence of the judiciary presupposes, in general, that judicial functions are exercised wholly autonomously, without the courts being subject to any hierarchical constraint or subordinate relationship and without taking orders or instructions from any source whatsoever, thus being protected from any external intervention or pressure liable to jeopardise the independent judgment of their members and to influence their decisions. Observance of the guarantees of independence and impartiality necessary under EU law requires rules in order to dispel any reasonable doubt in the minds of individuals as to the imperviousness of the body in question to external factors and its neutrality with respect to the interests concerned (see, to that effect, inter alia, judgments of 27 February 2018,   
Associação Sindical dos Juízes Portugueses  
, C-64/16, EU:C:2018:117, paragraph 44; of 25 July 2018,   
Minister for Justice and Equality (Deficiencies in the system of justice)  
, C-216/18 PPU, EU:C:2018:586, paragraph 63; of 24 June 2019,   
Commission  
 v   
Poland   
(Independence of the Supreme Court)  
, C-619/18, EU:C:2019:531, paragraph 72; and of 21 December 2021,   
Euro Box Promotion and Others  
, C-357/19, C-379/19, C-547/19, C-811/19, C-840/19, EU:C:2021:1034, paragraph 225).  
34      Accordingly, the reference in Article 55(3) of Regulation 2016/679 to processing operations carried out by courts ‘acting in their judicial capacity’ must be understood, in the context of that regulation, as not being limited to the processing of personal data carried out by courts in specific cases, but as referring, more broadly, to all processing operations carried out by courts in the course of their judicial activity, such that those processing operations whose supervision by the supervisory authority would be likely, whether directly or indirectly, to have an influence on the independence of their members or to weigh on their decisions are excluded from that authority’s competence.  
35      In that regard, while the nature and purpose of the processing carried out by a court relate principally to the examination of the lawfulness of that processing, they may constitute indicia that that processing falls within the exercise, by that court, of its ‘judicial capacity’.  
36      On the other hand, the question whether the processing has an explicit legal basis in domestic law or whether the personal data contained therein may lawfully be disclosed to third parties relates exclusively to the examination of the lawfulness of the processing, those elements being irrelevant to determining whether the supervisory authority is competent to ensure the supervision of that processing operation on the basis of Article 55 of Regulation 2016/679.  
37      As regards processing such as that at issue in the main proceedings, it must be held that, without prejudice to compliance with the substantive obligations laid down by Regulation 2016/679, the processing of personal data carried out by courts in the context of their communication policy on cases before them, such as those consisting in the temporary making available to journalists of documents from a court case file in order to enable them to cover it in the media, inter alia, falls outside the competence of the supervisory authority, pursuant to Article 55(3) of that regulation.  
38      The determination, having regard to the subject matter and context of a given case, of the information from a court case file that may be provided to journalists in order to enable them to report on the course of court proceedings or to shed light on one or other aspect of a decision delivered is clearly linked to the exercise, by such courts, of their ‘judicial capacity’, the supervision of which by an external authority would be liable to undermine, in general, the independence of the judiciary.  
39      In the light of all the foregoing considerations, the answer to the question referred is that Article 55(3) of Regulation 2016/679 must be interpreted as meaning that the fact that a court makes temporarily available to journalists documents from court proceedings containing personal data in order to enable them better to report on the course of those proceedings falls within the exercise, by that court, of its ‘judicial capacity’, within the meaning of that provision.  
   
Costs  
40      Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.  
On those grounds, the Court (First Chamber) hereby rules:  
Article 55(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as meaning that the fact that a court makes temporarily available to journalists documents from court proceedings containing personal data in order to enable them better to report on the course of those proceedings falls within the exercise, by that court, of its ‘judicial capacity’, within the meaning of that provision.