EN

Article 1.

Subject-matter and objectives

Article 1.

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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 1. Subject-matter and objectives

Recitals

(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.

(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.

(3) Directive 95/46/EC of the European Parliament and of the Council [4] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

[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 L 281, 23.11.1995, p. 31). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:1995:281:TOC

(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.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the

Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member 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.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(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/EC 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/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. 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.

(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.

(12) Article 16(2) TFEU mandates the European Parliament and the Council 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.

(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. 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. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. 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. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC [5].

[5] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2003:124:TOC

EN

Article 2.

Material scope

Article 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.

Recitals

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

Guidelines & Case Law

Documents

ICO, Frequently asked questions and answers about relevant filing systems, (2011).

Case Law

CJEU, Jehovan todistajat, C-25/17 (2018).

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;

Recitals

(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.

(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;

Recitals

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

Guidelines & Case Law

Documents

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

(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.

Recitals

(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 [7]. Member States may entrust competent authorities within the meaning of Directive (EU) 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.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation,

Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and 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. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

[7] 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 prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) 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.

Recitals

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council [6] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

[6] 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 L 8, 12.1.2001, p. 1). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2001:008:TOC

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 [17].

[17] OJ C 192, 30.6.2012, p. 7. https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:C:2012:192:TOC

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Recitals

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council [8], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

[8] 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 L 178, 17.7.2000, p. 1). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2000:178:TOC

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 2. Material scope

Recitals

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(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.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council [6] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

[6] 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 L 8, 12.1.2001, p. 1). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2001:008:TOC

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or

household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(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 [7]. Member States may entrust competent authorities within the meaning of Directive (EU) 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.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and 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. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

[7] 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 prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

(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.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council [8], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

[8] 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 L 178, 17.7.2000, p. 1). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2000:178:TOC

Guidelines & Case Law

Documents

EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (2019).

WP29, Opinion 5/2009 on online social networking (2009).

Case Law

CJEC, Criminal proceedings against Bodil Lindqvist, C-101/01 (2003).

CJEC, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07 (2008).

CJEU, *Ryneš/Úřad pro ochranu osobních údajů*, C-212/13 (2014).

CJEU, *Tietosuojavaltuutettu/Jehovan todistajat – uskonnollinen yhdyskunta*, C-25/17 (2018).

CJEU, *La Quadrature du Net et al./Premier ministre et al.*, C-511/18, C-512/18, C-520/18 (2020).

CJEU, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs*, C-623/17 (2020).

CJEU, *Data Protection Commissioner/Facebook Ireland Ltd and Schrems*, C-311/18 (2020).

EN

Article 3.

Territorial scope

Article 3.

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.

Recitals

(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.

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

Guidelines & Case Law

Documents

WP29, Update of Opinion on applicable law in light of the CJEU judgement in Google Spain (2010).

Case Law

CJEU, *Google Spain SL/Agencia española de protección de datos*, C-131/12 (2014):

> 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. (page 14)

CJEU, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16 (2018):

… 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. (page 14)

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

Recitals

(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. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Recitals

(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.

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.

Recitals

(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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 3. Territorial scope

Recitals

(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.

(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. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects 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.

Guidelines & Case Law

Documents

WP29, Update of Opinion on applicable law in light of the CJEU judgement in Google Spain (2010).

EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (2019).

EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (2021).

Case Law

CJEU, *Pammer and Hotel Alpenhof GesmbH/Reederei Karl Schlüter GmbH & Co. KG and Heller*, C-585/08 and C-144/09 (2010).

CJEU, *Google Spain SL/Agencia española de protección de datos*, C-131/12 (2014).

CJEU, *Verein für Konsumenteninformation/Amazon EU Sàrl*, C-191/15 (2015).

CJEU, *Weltimmo s.r.o./Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14 (2015).

CJEU, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16 (2018).

EN

Article 4.

Definitions

Article 4.

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;

Recitals

(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.

Guidelines & Case Law

Documents

Article 29 Working Party, Opinion Nº 4/2007 on the concept of personal data (2007).

Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines (2008).

> Data outlining the use of the service can be divided into different categories:
>
> - the query logs (content of the search queries, the date and time, source (IP address and cookie), the preferences of the user, and data relating to the user's computer);
> - data on the content offered (links and advertisements as a result of each query);
> - and data on the subsequent user navigation (clicks).
>
> Search engines may also process operational data relating to user data, data on registered users and data from other services and sources such as e-mail, desktop search, and advertising on third party websites.

An individual's *search history* is personal data if the individual to which it relates, is identifiable

Though *IP addresses* in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address.

When a cookie contains *a unique user ID*, this ID is clearly personal data.

ANNEX 1 contains example of data processed by search engines.

Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (2014).

Data Protection Commission (Ireland), Guidance Note: Anonymisation and Pseudonymisation (2019).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020):

9. There are two principal sources of location data available for modelling the spread of the virus and the overall effectiveness of confinement measures:
– location data collected by electronic communication service providers(such as mobile telecommunication operators) in the course of the provision of their service; and
– location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services,etc.).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020):

18. The term "*user*" is typically used to refer to individuals who are registered with the service, i.e. those who have an "account" or "profile". Many social media services can, however, also be accessed by individuals without having registered (i.e. without creating an account or profile). Such individuals are typically not able to make use of all of the same features or services offered to individuals who have registered with the social media provider. Both users and non-registered individuals may be considered "*data subjects*" within the meaning of Article 4(1) GDPR insofar as the individual is directly or indirectly identified or identifiable.

Case Law

CJEU, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs*, C-70/10 (2011).

CJEU, *Worten – Equipamentos para o Lar SA/Autoridade para as condições de trabalho*, C-342-12 (2013).

CJEU, *YS/Minister voor Immigratie, Integratie en Asiel*, C-141/12 and C-372/12 (2014).

CJEU, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources*, C-293/12 and C-594/12 (2014).

CJEU, *Breyer/Germany*, C-582/14 (2016).

CJEU, *Nowak/Data Protection Commissioner*, C-434/16 (2017).

CJEU, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Manni*, C-398/15 (2019).

(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;

Guidelines & Case Law

Documents

Article 29 Working Party, Opinion 2/2010 on behavioural advertising (2010):

> The behavioural advertising methods often entail the processing of personal data. This is due to various reasons:
>
> i) behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (through the cookie). The use of such devices with a unique identifier allows the tracking of users of a specific computer even when dynamic IP addresses are used. **In other words, such devices enable data subjects to be 'singled out', even if their real names are not known.**
>
> ii) Furthermore, the information collected in the context of behavioural advertising relates to, (i.e. is about) a person's characteristics or behaviour and it **is used to influence that particular person**. This view is further confirmed if one takes into account the possibility for profiles to be linked at any moment with directly identifiable information provided by the data subject, such as registration related information.

DPC (Ireland), Guidance for Organisations Accidentally in Receipt of Personal Data (2020):

> An organisation, whether in the public, private or voluntary sector, must be aware of the possibility of finding itself accidentally in possession of personal data. The broad definition of '**processing**' in Article 4(2) of the GDPR means that opening, transmitting, deleting or simply storing personal data that you have unintentionally acquired will bring the GDPR into play.

DPC (Ireland), Guidance for Individuals who Accidentally Receive Personal data (2020).

Case Law

CJEC, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07 (2008).

CJEC, *Lindqvist*, C-101/01 (2003).

CJEU, *Schwarz/Stadt Bochum*, C-291/12 (2013).

CJEU, *La Quadrature du Net et al./Premier ministre et al.*, C-511/18, C-512/18, C-520/18 (2020).

CJEU, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs*, C-623/17 (2020).

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(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;

Guidelines & Case Law

Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018):

> Profiling is composed of three elements:
>
> - it has to be an automated form of processing;
> - it has to be carried out on personal data; and
> - the objective of the profiling must be to evaluate personal aspects about a natural person.
>
> Article 4(4) refers to 'any form of automated processing' rather than 'solely' automated processing (referred to in Article 22). Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.
>
> Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.
>
> The GDPR says that profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse or make predictions about individuals. The use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person.
>
> A simple classification of individuals based on known characteristics such as their age, sex, and height does not necessarily lead to profiling. This will depend on the purpose of the classification. For instance, a business may wish to classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its clients without making any predictions or drawing any conclusion about an individual. In this case, the purpose is not assessing individual characteristics and is therefore not profiling.
>
> The GDPR is inspired by but is not identical to the definition of profiling in the Council of Europe Recommendation CM/Rec (2010)132 (the Recommendation), as the Recommendation excludes processing that does not include inference. Nevertheless

the Recommendation usefully explains that profiling may involve three distinct stages:

- data collection;
- automated analysis to identify correlations;
- applying the correlation to an individual to identify characteristics of present or future behaviour.

Controllers carrying out profiling will need to ensure they meet the GDPR requirements in respect of all of the above stages.

Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their:

- ability to perform a task;
- interests; or
- likely behaviour.

(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;

Recitals

(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.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for

attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

Guidelines & Case Law

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Guidelines & Case Law

Case Law

CJEU, *Tietosuojavaltuutettu/Jehovan todistajat – uskonnollinen yhdyskunta*, C-25/17 (2018).

(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;

Guidelines & Case Law

Document

Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines (2008).

> A *search engine provider* that processes user data including IP addresses and/or persistent cookies containing a unique identifier falls within the material scope of the definition of the *controller*, since he effectively determines the purposes and means of the processing.

Article 29 Working Party, Opinion 2/2010 on behavioural advertising (2010):

> When behavioural advertising entails the processing of personal data, ad network providers also play the role of **data controller**. Ad network providers have complete control over the purposes and means of the processing.

> However, the publishers' responsibility covers the first stage, i.e. the initial part of the data processing, namely the transfer of the IP address that takes place when individuals visit their websites. This is because the publishers facilitate such transfer and co-determine the purposes for which it is carried out, i.e. to serve visitors with tailored adverting. In sum, for these reasons, publishers will have some responsibility as **data controllers** for these actions.

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (2010).

ICO, Guidelines Data controllers and data processors (2014) – Guidelines by the British Supervisory Authority ICO.

CNIL, Guide for processors (2017) – Guidelines by the French Supervisory Authority CNIL.

European Data Protection Supervisor, *Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725* (2019).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

EDPB, *Guidelines 7/2020 on the Concepts of Controller and Processor in the GDPR* (2021).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

Data Protection Commission (Ireland), Data Protection Considerations Relating to Receivership (2020):

> The 'controller' of personal data is the entity that determines the 'purposes and means' of processing personal data – i.e. '**why**' and '**how**' the personal data is processed.

Case Law

CJEU, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16 (2018).

CJEU, *Fashion ID GmbH & Co. KG/Verbraucherzentrale NRW eV*, C-40/17 (2019).

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Guidelines & Case Law

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" *(2010).*

CNIL, Guide for processors (2017) – Guidelines from the French Supervisory Authority CNIL.

European Data Protection Supervisor, *Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725* (2019).

(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;

Recitals

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(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;

(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;

Recitals

(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.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only

to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Guidelines & Case Law

Document

EDPB, *Guidelines 5/2020 on Consent under Regulation 2016/679* (2020).

Case law

CJEU, *Schwarz/Stadt Bochum*, C-291/12 (2013).

CJEU, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV/Planet49 GmbH*, C-673/17 (2019).

(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;

Guidelines & Case Law

Article 29 Working Party, Guidelines on Personal Data Breach Notification Under Regulation 2016/679 (2018):

> In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles:
> – "Confidentiality breach" – where there is an unauthorised or accidental disclosure of, or access to, personal data.
> – "Integrity breach" – where there is an unauthorised or accidental alteration of personal data.
> – "Availability breach" – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

(13) '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;

Recitals

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person

which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

Guidelines & Case Law

Article 29 Working Party, Working Document on Genetic Data (2004).

(14) '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;

Guidelines & Case Law

To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of this characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is "resulting from specific technical processing relating to the physical, physiological or behavioural characteristics".The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual.

In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed "for the purpose of uniquely identifying a natural person".
To sum up, in light of Article 4.14 and 9, three criteria must be considered:

— **Nature of data**: data relating to physical, physiological or behavioural characteristics of a natural person,

— **Means and way of processing**: data "resulting from a specific technical processing",

— **Purpose of processing**: data must be used for the purpose to uniquely identifying a natural person.

EDPB, Guidelines 3/2019 on processing of personal data through video devices — 2019

Article 29 Working Party, Opinion 03/2012 on developments in biometric technologies (2012).

Article 29 Working Party, *Opinion 02/2012 on facial recognition in online and mobile services* (2012).

Article 29 Working Party, Working document on biometrics (2003).

(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;

Recitals

(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. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council [9] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

[9] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2011:088:TOC

Guidelines & Case Law

Documents

EDPB, Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak, (2020).

(16) 'main establishment' means:

Recitals

(36) The main establishment of a controller in the Union should be 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, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main

establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(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;

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(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;

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

Recitals

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

Recitals

(36) The main establishment of a controller in the Union should be 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, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(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.

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

Guidelines & Case Law

Documents

EDPB, Guidelines on relevant and reasoned objection under Regulation 2016/679 (2020).

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council [19];

[19] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2015:241:TOC

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 4. Definitions

Recitals

(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.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(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.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(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.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(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. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council [9] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk,

medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

[9] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2011:088:TOC

(36) The main establishment of a controller in the Union should be 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, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

EN

Article 5.

Principles relating to processing of personal data

Article 5.

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

Recitals

(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. 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. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

Guidelines & Case Law

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

(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');

Guidelines & Case Law

WP29, *Opinion 03/2013 on purpose limitation* (2013).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Guidelines & Case Law

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).

(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 insofar 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');

Guidelines & Case Law

Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines* (2008).

> In view of the initial explanations given by *search engine providers* on the possible purposes for collecting personal data, the Working Party does not see a basis for a retention period beyond *6 months*.
>
> In case search engine providers retain personal data longer than 6 months, they will have to demonstrate comprehensively that it is strictly necessary for the service.

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).

(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').

Guidelines & Case Law

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Recitals

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

Guidelines & Case Law

WP29, *Opinion 3/2010 on the principle of accountability* (2010).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 5. Principles relating to processing of personal data

Recitals

(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. 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. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

Guidelines & Case Law

Documents

ICO, *Accountability Framework*

WP29, *Opinion on data processing at work* (2017).

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

DPC (Ireland), Guidance for Individuals who Accidentally Receive Personal data (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

Case Law

ECHR, *López Ribalda v. Spain, nos 1874/13 and 8567/13* (2019).

Belgian DPA Fines Belgian Telecommunications Provider for Several Data Protection Infringements, (2020) – brief description in English.

Norwegian DPA, Issues fine to Aquateknikk AS (2021).

Norwegian DPA, Intention to issue € 10 million fine to Grindr LLC (2021).

EN

Article 6.

Lawfulness of processing

Article 6.

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;

Guidelines & Case Law

WP29, Guidelines on consent under Regulation 2016/679 (2018).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

EDPB, Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (2020).

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

(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;

Recitals

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

Guidelines & Case Law

EDPB, Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects (2019).

EDPB, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR (2020).

> Payment services are always provided on a contractual basis between the payment services user and the payment services provider.
>
> Controllers have to assess what processing of personal data *is objectively necessary* to perform the contract. Justification of the

necessity is dependent on:

- the nature of the service;
- the mutual perspectives and expectations of the parties to the contract;
- the rationale of the contract; and
- the essential elements of the contract.

The controller should be able to demonstrate how the main object of the specific contract with the data subject *cannot be performed* if the specific processing of the personal data in question does not occur. Merely *referencing or mentioning data processing in a contract is not enough* to bring the processing in question within the scope of Article 6(1)(b) of the GDPR.

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

Recitals

(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. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

Recitals

(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.

(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;

Recitals

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

Guidelines & Case Law

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

(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.

Recitals

(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. 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. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(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, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Guidelines & Case Law

Documents

WP29, Opinion on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" (2014).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020):

> 44. For what concerns the legitimate interest lawful basis, the EDPB recalls that in *Fashion ID*, the CJEU reiterated that in order for processing to rely on the legitimate interest, three cumulative conditions should be met, namely
>
> - the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed,
> - the need to process personal data for the purposes of the legitimate interests pursued, and
> - the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence.
>
> The CJEU also specified that in a situation of joint controllership *"it is necessary that each of those controllers should pursue a legitimate interest […] through those processing operations in order for those operations to be justified in respect of each of them"*.

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

Data Protection Commission (Ireland), Data Protection Considerations Relating to Receivership (2020).

EDPB, *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR* (2020).

The GDPR may allow for the processing of silent party data when this processing is necessary for purposes of the legitimate interests pursued by a controller or by a third party.

A lawful basis for the processing of silent party data by PISPs and AISPs – in the context of the provision of payment services under the PSD2 – could thus be the legitimate interest of a controller or a third party to perform the contract with the payment service user. The necessity to process personal data of the silent party is *limited* and determined by the *reasonable expectations of these data subjects.*

Effective and *appropriate measures* have to be established by all parties involved. In this respect, the controller has to establish the *necessary safeguards for the processing,* including *technical measures*. If feasible, also *encryption or other techniques* must be applied to achieve an appropriate level of security and data minimisation.

Case Law

CJEU, TK v Asociaţia de Proprietari bloc M5A-ScaraA, Case C-708/18 (2018).

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Recitals

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity 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.

(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. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. 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. 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.

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. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

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.

Recitals

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

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:

Guidelines & Case Law

Documents

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

(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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 6. Lawfulness of processing

Recitals

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity 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.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(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 [10] 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.

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:1993:095:TOC

(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.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(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. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(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. 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. 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. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(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, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

(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. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. 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. 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.

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. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(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.

Guidelines & Case Law

Documents

Article 29 Working Party, Opinion 6/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC (2014).

EDPB, *Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (2017).

WP29, *Opinion on data processing at work* (2017).

EDPB, *Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data* (2019).

EDPB, Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects (2019).

Data Protection Commission of Ireland, Guidance Note: Legal Bases for Processing Personal Data (2019).

Data Protection Commission (Ireland), Data Protection Considerations Relating to Receivership (2020).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

Case Law

CJEC, *Rechnungshof/Österreichischer Rundfunk*, C-465/00, C-138/01 and C-139/01 (2003).

CJEC, *Huber/Germany*, C-524/06 (2008).

CJEU, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs*, C-70/10 (2011).

CJEU, *Google Spain SL/Agencia española de protección de datos*, C-131/12 (2014).

ECHR, Antović and Mirković v. Montenegro, no. 70838/13 (2017).

ECHR, *López Ribalda v. Spain, nos 1874/13 and 8567/13* (2019).

Belgian DPA Fines Belgian Telecommunications Provider for Several Data Protection Infringements (2020). Brief description in English.

Norwegian DPA, issues fine to Aquateknikk AS (2021).

EN

Article 7.

Conditions for consent

Article 7.

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.

Recitals

(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 [10] 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.

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:1993:095:TOC

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.

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.

Recitals

(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.

(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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 7. Conditions for consent

Recitals

(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.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(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 [10] 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.

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:1993:095:TOC

(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.

Guidelines & Case Law

Documents

Article 29 Working Party, Opinion 4/2012 on Cookie Consent Exemption (2012).

Article 29 Working Party, Working Document 2/2013 Providing Guidance on Obtaining Consent for Cookies (2013).

EDPB, *Guidelines 5/2020 on Consent under Regulation 2016/679* (2020).

CNIL, Guidelines on Cookies and Tracking Devices (in French) (2019).

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).

Case Law

CJEU, Judgment in Planet 49 Gmbh, Case C-673/17 (2019).

Belgian DPA Fines Belgian Telecommunications Provider for Several Data Protection Infringements, (2020). Brief description in English.

CJEU, *Data Protection Commissioner/Facebook Ireland Ltd and Schrems*, C-311/18 (2020).

CNIL, *Cookies :* sanction de 35 millions d'euros à l'encontre d'AMAZON EUROPE CORE *and* sanction de 60 millions d'euros à l'encontre de GOOGLE LLC et de 40 millions d'euros à l'encontre de GOOGLE IRELAND LIMITED (2020).

EN

Article 8.

Conditions applicable to child's consent in relation to information society services

Article 8.

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Guidelines & Case Law

Documents

Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679* (2018).

> The inclusion of the wording '**offered directly to a child**' indicates that Article 8 is intended to apply to some, not all information society services. In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply.

Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679* (2018).

> Where a data controller is targeting children[16] or is, or should be, aware that their goods/services are particularly utilised by children (including where the controller is relying on the consent of the child)[17], it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them.[18] A useful example of child-centred language used as an alternative to the original legal language can be found in the "UN Convention on the Rights of the Child in Child Friendly Language".[19]

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

Guidelines & Case Law

Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679, WP259 rev.01* (2018):

> What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR. Trusted third party verification services may offer solutions which minimise the amount of personal data the controller has to process itself.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 8. Conditions applicable to child's consent in relation to information society services

Recitals

(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.

Guidelines & Case Law

Documents

Article 29 Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)* (2009).

EDPB, *Guidelines 5/2020 on Consent under Regulation 2016/679* (2020).

ICO, Age Appropriate Design: A Code of Practice for Online Services (2020).

Case Law

CJEU, *Data Protection Commissioner/Facebook Ireland Ltd and Schrems*, C-311/18 (2020).

EN

Article 9.

Processing of special categories of personal data

Article 9.

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.

Recitals

(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 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.

Guidelines & Case Law

Documents

Article 29 Working Party, *Opinion 2/2012 on Facial Recognition in Online and Mobile Services* (2012).

Article 29 Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* (2012).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020):

> If a social media provider or a targeter uses observed data to categorise users as having certain religious, philosophical or political beliefs-regardless of whether the categorization is correct/true or not-this categorisation of the user must obviously be seen as processing of special category of personal data in this context. As long as the categorisation enables targeting based on special category data, it does not matter how the category is labelled.

EDPB, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR (2020).

> *Financial transactions can reveal sensitive information about individual data subject*, including those related to special categories of personal data. For example, *political opinions and religious beliefs* may be revealed by donations made to political parties or organisations, churches or parishes. *Trade union membership* may be revealed by the deduction of an annual membership fee from a person's bank account. *Personal data concerning health* may be gathered from analysing medical bills paid by a data subject. Finally, information on certain purchases may reveal *information concerning a person's sex life or sexual orientation.*
>
> Moreover, through the sum of financial transactions, different kinds of behavioural patterns could be revealed, including special categories of personal data and additional services that are facilitated by account information services might rely on profiling as defined by article 4 (4) of the GDPR. Therefore, the chances are considerable that *a service provider processing information on financial transactions of data subjects also processes special categories of personal data.*

2. Paragraph 1 shall not apply if one of the following applies:

Recitals

(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, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council [11], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

[11] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2008:354:TOC

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(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;

(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 in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(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 and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

Guidelines & Case Law

EDPB, Guidelines 8/2020 on the targeting of social media users (2020):

> The word "manifestly" implies that there must be a high threshold for relying on this exemption.The EDPB notes that the presence of a single element may not always be sufficient to establish that the data have been "manifestly" made public by the data subject. In practice,a combination of the following or other elements may need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public, and a case-by-case assessment is needed. The following elements may be relevant to help inform this assessment:
>
> - the default settings of the social media platform (i.e. whether the data subject took a specific action to change these default private settings into public ones); or
> - the nature of the social media platform (i.e. whether this platform is intrinsically linked with the idea of connecting with close acquaintances of the data subject or creating intimate relations (such as online dating platforms), or if it is meant to provide a wider scope of interpersonal relations, such as professional relations, or microblogging, etc… ; or
> - the accessibility of the page where the sensitive data is published (i.e. whether the information is publically accessible or if, for instance, the creation of an account is necessary before accessing the information); or
> - the visibility of the information where the data subject is informed of the public nature of the information that they publish (i.e. whether there is for example a continuous banner on the page, or whether the button for publishing informs the data subject that the information will be made public…); or
> - if the data subject has published the sensitive data himself/herself, or whether instead the data has been published by a third party (e.g. a photo published by a friend which reveals sensitive data) or inferred.
>
> The EDPB notes that the presence of a single element may not always be sufficient to establish that the data have been "manifestly" made public by the data subject. In practice,a combination of these or other elements may need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public.

(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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Guidelines & Case Law

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

(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;

Guidelines & Case Law

Legislation

Regulation (EC) No 1338/2008 on Community Statistics on Public Health and Health and Safety at Work, OJEU L 354, 31 December 2008, p. 70.

Documents

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on 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.

Guidelines & Case Law

Document

EDPB, *Opinion 3/2019 Concerning the Questions and Answers on the Interplay Between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (art. 70.1.b))* (2019).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

Legislation

Regulation (EU) No 536/2014 on Clinical Trials on Medicinal Products for Human Use, OJEU L 158, 27 May 2014, p. 1.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 9. Processing of special categories of personal data

Recitals

(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 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.

(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, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council [11], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

[11] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2008:354:TOC

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

Guidelines & Case Law

Documents

Article 29 Working Party, Opinion 2/2010 on behavioural advertising (2010):

> Any possible targeting of data subjects based on sensitive information opens the possibility of abuse. Furthermore, given the sensitivity of such information and the possible awkward situations which may arise if individuals receive advertising that reveals, for example, sexual preferences or political activity, offering/using interest categories that would reveal sensitive data **should be discouraged**.
>
> In this context, the only available legal ground that would legitimize the data processing would be explicit, separate prior opt-in **consent.** The requirement for a separate, affirmative prior indication of the data subjects' agreement means that in no case would an opt-out consent mechanism meet the requirement of the law. It also means that such consent **could not be obtained through browser settings**. To lawfully collect and process this type of information, ad network providers would have to set up mechanisms to obtain explicit prior consent, **separate from other consent obtained for processing in general**.

EDPB, *Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (2017).

WP29, *Opinion on data processing at work* (2017).

European Commission, Commission Guidance on the application of Union data protection law in the electoral context, *A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018.*

EDPB, *Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data* (2019).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

EDPB, Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (2020).

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data

protection Brussels (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

Case Law

Grainger Plc v. *Nicholson*, [2010] ICR 360.

CJEC, *Lindqvist*, C-101/01 (2003).

Eur. Court HR (Grand Chamber), *López Ribalda* v. *Spain*, nos. 1874/13 and 8567/13 (2019).

Eur. Court HR, *Gaughran* v. *United Kingdom*, no. 45245/15 (2020).

EN

Article 10.

Processing of personal data relating to criminal convictions and offences

Article 10.

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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 10. Processing of personal data relating to criminal convictions and offences

Guidelines & Case Law

Legislation

Directive (EU) 2016/680 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, OJEU L 119, 4 May 2016, p. 89.

EN

Article 11.

Processing which does not require identification

Article 11.

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 11. Processing which does not require identification

Recitals

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

EN

Article 12.

Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 12.

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.

Recitals

(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.

Guidelines & Case Law

Documents

Article 29 Working Party, Opinion 2/2010 on behavioural advertising (2010):

> The obligation to provide the necessary information and obtain data subjects' consent ultimately lies with the entity that sends and reads the cookie. In most cases, this is the ad network provider. When publishers are joint-controllers, for example in those cases where they transfer directly identifiable information to ad network providers, they are also bound by the obligation to provide information to data subjects about the data processing.

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.

Recitals

(59) 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. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

Guidelines & Case Law

Documents

Spanish Data Protection Agency (AEPD), Guide on use of cookies (2021).

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. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. 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.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

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.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject

Recitals

(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.

(59) 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. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

Guidelines & Case Law

Document

Article 29 Working Party, Guidelines on Transparency Under Regulation 2016/679 (2018).

Information Commissioner's Office, *Right of Access* (2020).

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

Case Law

CJEU, *Smaranda Bara e.a./Președintele Casei Naționale de Asigurări de Sănătate*, C-201/14 (2015).

ECHR, *López Ribalda v. Spain, nos 1874/13 and 8567/13* (2019).

Belgian DPA Fines Belgian Telecommunications Provider for Several Data Protection Infringements (2020) – brief description in English.

EN

Article 13.

Information to be provided where personal data are collected from the data subject

Article 13.

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:

Recitals

(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. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2018):

> This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address etc.).

(b) the contact details of the data protection officer, where applicable;

Guidelines & Case Law

Article 29 Working Party, Guidelines on Data Protection Officers (DPOs) (2017):

> The contact details of the DPO should include information allowing data subjects and the supervisory authorities to reach the

DPO in an easy way (a postal address, a dedicated telephone number, and/or a dedicated e-mail address). When appropriate, for purposes of communications with the public, other means of communications could also be provided, for example, a dedicated hotline, or a dedicated contact form addressed to the DPO on the organisation's website.

Article 37(7) does not require that the published contact details should include the name of the DPO. Whilst it may be a good practice to do so, it is for the controller or the processor and the DPO to decide whether this is necessary or helpful in the particular circumstances.

[…]

As a matter of good practice, the WP29 also recommends that an organisation informs its employees of the name and contact details of the DPO. For example, the name and contact details of the DPO could be published internally on organisation's intranet, internal telephone directory, and organisational charts.

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2018):

In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security measures based on Article 6.1 is processed, where applicable the relevant Union or Member State law under which the processing is carried out should be specified.

(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;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the controller can also provide the data subject with the information from the balancing test, which must be carried out to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data. To avoid information fatigue, this can be included within a layered privacy statement/ notice (see paragraph 35). In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority.

(e) the recipients or categories of recipients of the personal data, if any;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

The term "recipient" is defined in Article 4.9 as "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, **whether a third party or not**" [emphasis added]. As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article

45/ binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.

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:

Recitals

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> This is linked to the data minimisation requirement in Article 5.1(c) and storage limitation requirement in Article 5.1(e). The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020):

> Storage limitation should consider the true needs and the medical relevance (this may include epidemiology-motivated considerations like the incubation period,etc.) and personal data should be kept only for the duration of the COVID-19 crisis. Afterwards,as a general rule,all personal data should be erased or anonymised.

(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;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right. […] In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.64 In relation to the right to portability, see WP29 Guidelines on 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;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.

(d) the right to lodge a complaint with a supervisory authority;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> This information should explain that, in accordance with Article 77, a data subject has 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 of an alleged infringement of the GDPR.

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> For example in an employment context, it may be a contractual requirement to provide certain information to a current or prospective employer. Online forms should clearly identify which fields are “required”, which are not, and what will be the consequences of not filling in the required fields.

(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.

Guidelines & Case Law

Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (2018):

> Given the core principle of transparency underpinning the GDPR, controllers must ensure they explain clearly and simply to individuals how the profiling or automated decision-making process works.
> In particular, where the processing involves profiling-based decision making (irrespective of whether it is caught by Article 22

provisions), then the fact that the processing is for the purposes of both (a) profiling and (b) making a decision based on the profile generated, must be made clear to the data subject.

Recital 60 states that giving information about profiling is part of the controller's transparency obligations under Article 5(1)(a). The data subject has a right to be informed by the controller about and, in certain circumstances, a right to object to 'profiling', regardless of whether solely automated individual decision-making based on profiling takes place.

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 13. Information to be provided where personal data are collected from the data subject

Recitals

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(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. 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. 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. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or

processing activities to which the request relates.

Guidelines & Case Law

Document

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2018)

EDPB, Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (2020).

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

Case Law

CJEU, *College van burgemeester en wethouders van Rotterdam/Rijkeboer*, C-553/07 (2009).

CJEU, *YS/Minister voor Immigratie, Integratie en Asiel*, C-141/12 and C-372/12 (2014).

CJEU, *ClientEarth/European Food Safety Authority*, C-615/13 P (2015).

CJEU, *Nowak/Data Protection Commissioner*, C-434/16 (2017).

ECHR, *López Ribalda v. Spain, nos 1874/13 and 8567/13* (2019).

Belgian DPA Fines Belgian Telecommunications Provider for Several Data Protection Infringements (2020). Brief description in English.

EN

Article 14.

Information to be provided where personal data have not been obtained from the data subject

Article 14.

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. 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:

(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) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) 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 and to object to processing as well as the right to data portability;

(d) where 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;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(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.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the

objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 14. Information to be provided where personal data have not been obtained from the data subject

Guidelines & Case Law

Document

Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679* (2018).

European Commission, Commission Guidance on the application of Union data protection law in the electoral context, *A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018.*

EDPB, Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

Case Law

CJEU, *College van burgemeester en wethouders van Rotterdam/Rijkeboer*, C-553/07 (2009).

CJEU, *YS/Minister voor Immigratie, Integratie en Asiel*, C-141/12 and C-372/12 (2014).

CNIL, *Cookies :* sanction de 35 millions d'euros à l'encontre d'AMAZON EUROPE CORE *and* sanction de 60 millions d'euros à l'encontre de GOOGLE LLC et de 40 millions d'euros à l'encontre de GOOGLE IRELAND LIMITED (2020).

EN

Article 15.

Right of access by the data subject

Article 15.

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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 15. Right of access by the data subject

Recitals

(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. 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. 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. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

Guidelines & Case Law

Guidelines

Information Commissioner's Office, *Right of Access* (2020).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

EDPB, *Guidelines 01/2022on data subject rights – Right of access* (2022).

Case Law

CJEU, *College van burgemeester en wethouders van Rotterdam/Rijkeboer*, C-553/07 (2009).

CJEU, *Nowak/Data Protection Commissioner*, C-434/16 (2017).

EN

Article 16.

Right to rectification

Article 16.

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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 16. Right to rectification

Expert commentary

The Council of Europe recommended, in 1973, that "*inaccurate information*" should be corrected in the context of data compiled in electronic data banks (*Resolution on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector*). So, it is not surprising that the European Union 2016 *General Data Protection Regulation* provides for a "*right to rectification*". The surprise comes from the absence of guidance regarding the rights and responsibilities related to the exercise of that right.

A person may ask the controller to rectify "*inaccurate personal data*" concerning him or her. The controller has the obligation to proceed to that rectification "*without undue delay*" and free of charge (recital 59). The right extends to complete incomplete data, a person being allowed to produce a supplementary statement to this end. In that event, the controller can accept or refuse the modification depending on the purposes of the processing.

The GDPR does not define what are "*inaccurate*" personal data, but the Court of Justice of the European Union excludes that the right to rectification extends to allowing a person to correct an incorrect answer to an exam (Nowak). It does not mean that a person cannot ask to rectify an answer or an examiner's comment regarding the exam that does not accurately reflect the original answer of the candidate. It can happen if, for example, copies were mixed up and another candidate's answers were ascribed to the candidate concerned (Nowak).

The possibility to complete or rectify inaccurate or incomplete information can also be invoked in the context of profiling, i.e. when a company establishes profiles of employees or users for different reasons (advertising, marketing, work performance, and so on). It is the case where it uses personal data, usually through automated processing, to make decisions concerning them or to analyze or predict their personal preferences, behaviors or attitudes [article 4 (4) and recital 24].

Author

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

A "*profiled*" person may use her/his right of access (article 15) to learn what information was used to create the profile and the content of the profile itself. The "*right to rectification*" would allow her/him to amend, change or update any inaccuracies discovered (*Guidelines on Automated individual decision-making and Profiling*). A person might have been included in a category, for example, that does not correspond to her/his ability to perform a task at work or is irrelevant to her/his health condition. The person may challenge the accuracy of the information used and the end result, that is to say, the profile itself (*Guidelines on Automated individual decision-making and Profiling*).

Expert commentary

Data Subject Request Letter Sample

Concern: Request to rectify inaccurate personal data

Dear Madam, Dear Sir,

You have data concerning me that are inaccurate.

More specifically, the following data are incorrect:

[*My name* | *My email address* | *My personal address* | *My phone number* | *etc.*]

Pursuant to Article 16 of the *General Data Protection Regulation* (GDPR), please correct the data as follows:

[*Accurate information*]

Thank you for confirming as soon as possible that you have made the rectification, and in any event within one month of the receipt of my request, according to Article 12(3) of the GDPR.

Please, notify this request for rectification to every recipient to whom you have disclosed my personal data, as provided for by Article 19 of the GDPR.

Sincerely,

Author

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

[Your name]

Expert commentary

Data Subject Request Letter Sample

Concern: Request to rectify incomplete personal data

Dear Madam, Dear Sir,

You have data concerning me that are incomplete.

More specifically, the following data have to be completed:

[*My name* | *My email address* | *My personal address* | *My phone number* | *etc.*]

Pursuant to Article 16 of the *General Data Protection Regulation* (GDPR), please complete the data as follows:

[*Complete information*]

Thank you for confirming as soon as possible that you have made the rectification, and in any event within one month of the receipt of my request, according to Article 12(3) of the GDPR.

Please, notify this request for rectification to every recipient to whom you have disclosed my personal data, as provided for by Article 19 of the GDPR.

Sincerely,

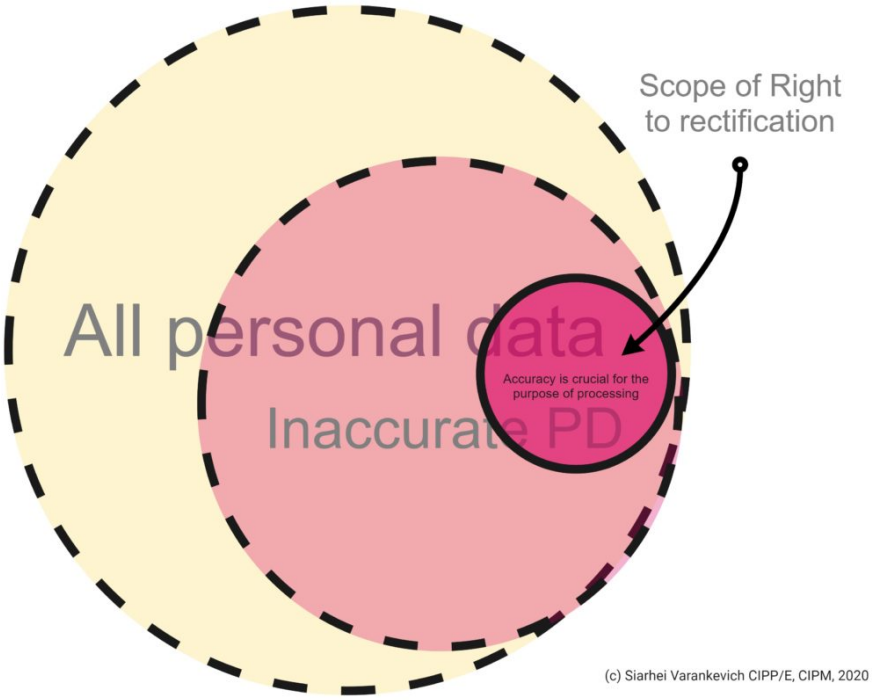
Data Subject

Author

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

Expert commentary

Author



Siarhei Varankevich
CIPP/E, CIPM, CIPT, MBA, FIP
Co-Founder & CEO of Data Privacy Office LLC. Data Protection Trainer and Principal Consultant

Guidelines & Case Law

Case Law

CJEU, *Nowak/Data Protection Commissioner*, C-434/16 (2017).

EN

Article 17.

Right to erasure (‘right to be forgotten’)

Article 17.

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;

(b) for compliance with a legal obligation which requires processing by Union or Member State law 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;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 17. Right to erasure (‘right to be forgotten’)

Recitals

(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. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. 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, 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, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(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.

Guidelines & Case Law

Documents

Article 29 Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain Inc. v. Agencia Española de protección de datos (AEPD) and Mario Costeja González C-131/12*

(2014).

EDPB, *Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR (part 1)* (2019).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

Case law

CJEU, *Google Spain SL/Agencia española de protección de datos*, C-131/12 (2014).

CJEU, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Manni*, C-398/15 (2019).

CJEU, *GC e.a./Commission nationale de l'informatique et des libertés*, C-136/17 (2019).

CJEU, *Google LLC/Commission nationale de l'informatique et des libertés*, C-507/17 (2019).

EN

Article 18.

Right to restriction of processing

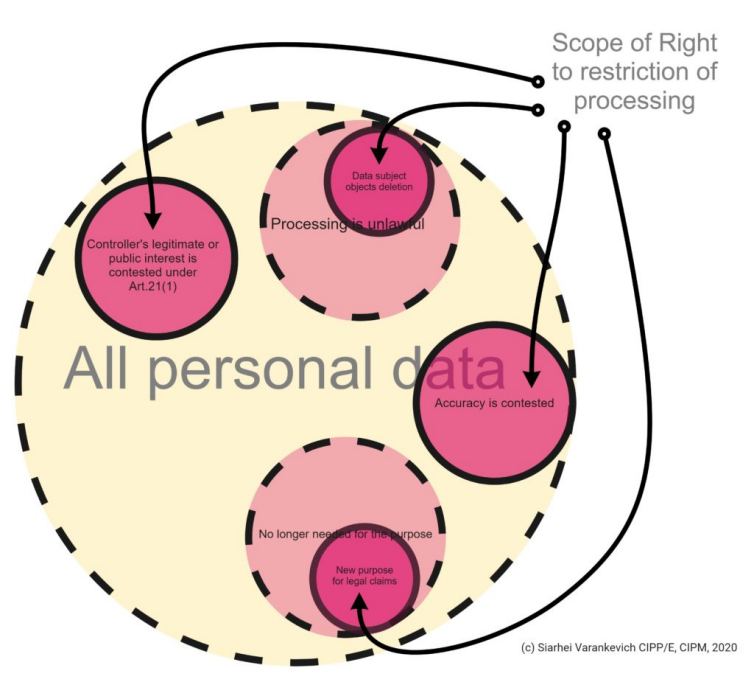
Article 18.

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

Expert commentary

Author

Siarhei Varankevich
CIPP/E, CIPM, CIPT, MBA, FIP
Co-Founder & CEO of Data Privacy Office LLC.
Data Protection Trainer and Principal Consultant


Scope of Right to restriction of processing
Data subject objects deletion
Processing is unlawful
Controller's legitimate or public interest is contested under Art.21(1)
All personal data
Accuracy is contested
No longer needed for the purpose
New purpose for legal claims
(c) Siarhei Varankevich CIPP/E, CIPM, 2020

(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.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 18. Right to restriction of processing

Expert commentary

Author

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

The right to restriction of processing is one of the eight rights granted by the GDPR, but it is not the easiest one to understand at first glance. It can be summed up as an obligation on behalf of the controller to retain data, but they can neither be processed in any other manner nor modified.

The right is exercised in cases where there is no clear indication of whether personal data will be deleted on a precise legal ground or when. It is especially useful when the right to erasure (article 17) cannot be invoked immediately, if the organization has a legal obligation to retain the data, for example.

A person has a limited right to restrict the processing of her/his data under four scenarios:

- if the accuracy of the concerned data is challenged;
- if the processing of the data was unlawful but the person opposed to their deleting;
- if the data are needed to establish, exercise or fight a legal claim; or
- if a person exercised her/his right to object (article 21) but the controller claimed "*compelling legitimate*" grounds for the processing.

Paragraph 2 of the provision entails the consequences of exercising one's right to restriction of processing. Aside from storage, the personal data cannot be processed anymore except i) with the consent of the person concerned; ii) in actions related to a legal claim; iii) for the protection of the rights of other persons (recital 73); or iv) if important public interests are involved (recital 73).

The GDPR text does not specify how to restrict the processing of personal data in cases where a person asks to, but recital 67 suggests a non-exhaustive list of methods to achieve that goal. The data can be moved temporarily to another processing system, access to specific data can be restricted or data

can be temporarily unpublished from a website. Technical means must ensure that data are not processed or changed where automated filing systems are concerned. The restrictions should be clearly mentioned whatever method is preferred (recital 67).

The duration of the restriction is also unclear. The European legal texts mention that data must not be processed "*for a period enabling the controller to verify [their] accuracy*", for example, or "*pending the verification*" whether exists a legitimate ground overriding a person's objection to processing. The time during which data cannot be processed will be a question of facts or of individual situations. One thing is clear though: a person must be informed before the restriction of processing is lifted.

Expert commentary

Data Subject Request Letter Sample

Concern: Request to restrict the processing of my personal data

Dear Madam, Dear Sir,

I am entitled to ask you to restrict the processing of my personal data under Article 18(1) of the *General Data Protection Regulation* (GDPR).

The requested restriction of processing is based on the fact that [*I contest the accuracy of my personal data that you hold*] [*you unlawfully processed my personal data and I am opposed to their deletion*] [*I need you to keep my personal data while I establish | exercise | prepare a defense to a legal claim*] [*I have objected to the processing of my personal data pursuant to Article 21(1) of the GDPR*].

You have the legal obligation to retain my personal data during that period, but you can neither process them in any other manner nor modified them.

Thank you for confirming as soon as possible that you have restricted the processing of my personal data, and in any event within one month of the receipt of my request, according to Article 12(3) of the GDPR.

In the absence of any action taken upon my request in a timely manner, I

Author

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

reserve my right to lodge a complaint with the relevant supervisory authority and seek judicial remedy.

Sincerely,

Data Subject

Recitals

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

EN

Article 19.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

Article 19.

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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 19. Notification obligation regarding rectification or erasure of personal data or restriction of processing

Expert commentary

Article 19 includes a notification obligation, which should not be confused with the specific personal data breach notification obligation (article 33). It is a mechanism that gives full effect to other provisions of the *General Data Protection Regulation*, ensuring that third parties are informed about actions taken by the controller regarding personal data (recital 66).

After a person has exercised her/his right to **rectification** (article 16), **erasure** (article 17) or **restriction of processing** (article 18), the controller must inform all parties ("*recipients*") to whom s/he has disclosed data. The provision should be read as referring to all forms of communication of personal data, like "*disclosure by transmission, dissemination or otherwise making available*" [article 4 (2)]. The recipient identified in the text of the provision comprises natural or legal persons, public authorities, agencies or bodies [article 4 (9)]. They are not limited to external parties, they encompass in-house persons, departments or services.

There is a limit to the general obligation imposed on the controller to inform recipients: her/his responsibility ends where it proves impossible to do so or it involves "*disproportionate effort*" on her/his part. Articles 14 (5) b) and 34 (3) c) of the GDPR uses the same wording ("*disproportionate effort*"), but the Court of Justice of the European Union did not interpret the meaning of the expression yet.

However, the Court of Appeal of England and Wales clarified similar wording in the former domestic *Data Protection Act 1998* [article 8(2)(a)] before the entry into force of the GDPR. The case involved a data access request and the "*disproportionate effort*" exception to refuse to comply with the demand. The judge left it to an appreciation of facts of each particular case to balance the effort involved in finding and supplying the information against the potential benefit it might bring to the person requesting data (*Dawson-Damer* v. *Taylor Wessing LLP*).

Author

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

The "*disproportionate effort*" exception of article 19 should not be read as a way to get around the provisions of the GDPR. It should not be invoked, for example, if the "*disproportionate effort*" results of the number of recipients to whom the controller disclosed personal data. The burden of proving that the request would involve "*disproportionate effort*" should rest on the controller's shoulders. S/he should demonstrate that s/he took "*reasonable steps*" to inform recipients of personal data, "*taking into account available technology and the means available*" (recital 66).

The controller should not be allowed to invoke inadequate information management systems or poor practices to refuse to inform recipients, as they can be viewed as a breach of her/his obligations under the GDPR to implement data protection by design and by default (article 25).

The goal of the provision may be evaded nonetheless by the recipient as s/he is formerly under no legal obligation to use the controller's information. The drafters of the European regulation seem to have ignored this scenario, letting recipients decide whether or not they will give effect to the request of the controller.

As the concerned person may ask to be informed about the identity of the recipients, s/he may have to exercise her/his rights to rectification, erasure or restriction of processing by contacting directly each identified recipient. It would be a shift in the notification obligation from the controller to the data subject, although the latter has not decided to share her/his information with other recipients.

Guidelines & Case Law

Case Law

England and Wales Court of Appeal (EWCA), *Dawson-Damer* v. *Taylor Wessing LLP*, EWCA Civ 74 (2017).

EN

Article 20.

Right to data portability

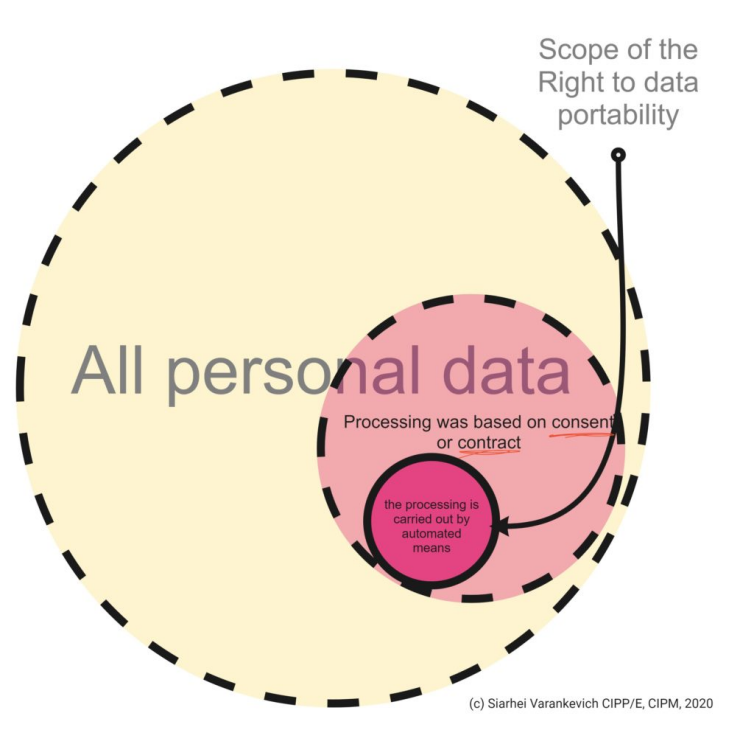
Article 20.

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

Expert commentary

Author

Siarhei Varankevich
CIPP/E, CIPM, CIPT, MBA, FIP
Co-Founder & CEO of Data Privacy Office LLC.
Data Protection Trainer and Principal Consultant


Scope of the Right to data portability
All personal data
Processing was based on consent or contract
the processing is carried out by automated means
(c) Siarhei Varankevich CIPP/E, CIPM, 2020

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 20. Right to data portability

Expert commentary

Author

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

The right to data portability is presented primarily as a way to support "*user choice, user control, and user empowerment*" (*Guidelines on the Right to Data Portability*), as it aims at reinforcing an individual's control over her/his personal information (recital 68). Data portability allows users to receive a copy of their personal data and can be seen in that sense as an extension of the right of access (article 15). It can also help them to switch services without losing their data, enabling users to transfer their information from one service to a potentially better one.

Article 20 provides for a general right to data portability, which may be decomposed into two separate rights: i) a right to receive one's personal data "*in a structured, commonly used and machine-readable format*"; and ii) a right to transmit the received data without interference. Portability can be invoked if the following conditions are respected:

- data has been collected based on **consent** [article 6 (1) (a) or 9 (2) (a)] or on a **contract** [article 6 (1) (b)]; and
- they were processed by **automated means**, which excludes most paper files (*Guidelines on the Right to Data Portability*).

What are the data concerned by the portability right? Article 20 says it is the data "*provided*" by a person. The *Guidelines on the Right to Data Portability* specifies that this word must be interpreted broadly. It recommends that data derived from the activities of users (logs, browsing history, search activities, location, and so on) should be treated as data "*provided*" by a user. Therefore, the right covers not only the data actively and directly volunteered by users, but also those generated by their activity while using the application, device or service in question. The official interpretation extends the reach of the right to data portability beyond the text of the article itself and the legislative intent of the Council and the Parliament, some critics say.

Data concerned by the provision are only "*personal data*", within the meaning of article 4 (1), which excludes anonymous data and data that are not related to a user (*Guidelines on the Right to Data Portability*). It should also be emphasized that the right to data portability must be regarded in the context of the *General Data Protection Regulation*. It concerns "*personal data*" and not data in general. A playlist from a streaming service, for example, contains the listening preferences of a user and is thus included in the scope of the right but the songs themselves are not.

The right to data portability cannot, as a rule, affect other people's rights (recital 68). The guarantee aims at avoiding the processing of third parties' personal data without a legal basis while allowing a person to exercise her/his right to data portability. However, there are limits to this exception. If, for example, a person requests his/her calling data, the data might includes third parties' information related to incoming and outgoing calls (like phone numbers). These data should be considered for the portability right as they also concern the person who requests the data (*Guidelines on the Right to Data Portability*). One can argue that the transfer does not affect third parties' rights more than the initial processing, explaining the existence of this limit to safeguarding the rights and freedoms of others.

Article 20 prescribes that data should be communicated "*in a structured, commonly used and machine-readable format*", but falls short of defining precisely the outline of these requirements. A machine-readable format is defined in a European directive as a format "*that is structured in such a way that software applications can easily identify, recognise and extract specific data from it*" (*Directive 2013/37/EU*).

"*Structured*" could refer to an obligation to organize the information in such a way that it can be easily accessible to users. They should not have to dig into the document or file provided to find the expected data. Information should be classified or categorized systematically in a comprehensible manner and they should be offered "*in a format which supports re-use*" (*Guidelines on the Right to Data Portability*).

The expression "*commonly used*", read in conjunction with recital 68, seems to refer to the concept of "*interoperability*". Indeed, recital 68 completes the text of the article adding a requirement that data should be made available in an "*interoperable*" format. It states that "*controllers should be encouraged to develop interoperable formats that enable data portability*", but it does not go as far as requesting that controllers adopt or maintain technically compatible

processing systems.

Even if it was adopted as one of the eight rights guaranteed by the GDPR, the right to data portability may be looked at first and foremost as a regulatory tool to stimulate competition and innovation in the European internal market. It may be potentially thought of as an economic incentive to promote the free flow of information and competitiveness between service providers.

The right to transmit received data to another controller depends almost solely on innovation. Could the requirement of being able to transfer data "*without hindrance*" be read as an obligation to develop such systems? The *Guidelines on the Right to Data Portability* specify that "*hindrance*" comprehends "*legal, technical or financial obstacles*" if they refrain or slow down access, transmission or reuse of data. The *Guidelines* go as far as classifying the lack of interoperability as an example of such hindrance. It should be mentioned though that article 20 poses one condition to the exercise of the right to transfer data: it must be technically feasible.

Data portability poses a challenge to information technology companies as they are generally not ready technically to answer such a demand. The technology giant companies partnered to develop new standards to make it technically possible to transfer data from one service to another (Data Transfer Project), but it is still in the process of being elaborated. The European Union granted a right which can push innovation, but cannot be fully respected in the present state of the art. Technical developments are still in their infancy and it seems almost premature to label data portability as a "*right*".

Expert commentary

Data Subject Request Letter Sample

Author

Concern: Exercise my right to data portability

Dear Madam, Dear Sir,

I would like to exercise my right to data portability under Article 20 of the *General Data Protection Regulation* (GDPR).

I would like to obtain a copy of all my personal data [*in a structured, commonly used and machine-readable format*] [*transferred to XXX*].

Personal data requested include information I have provided to your [*company* | *organization* | *etc.*] and information that your [*company* | *organization* | *etc.*] has gathered by monitoring my activity while using your [*app* | *device* | *service* | *website* | *etc.*].

Thank you for providing me with an answer as soon as possible, and in any event within one month of the receipt of my request, according to Article 12(3) of the GDPR.

In the absence of any action taken upon my request in a timely manner or in the event of an incomplete answer, I reserve my right to lodge a complaint with the relevant supervisory authority and seek judicial remedy.

Sincerely,

Data Subject

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

Recitals

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data 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 an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for

as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

Guidelines & Case Law

Documents

Article 29 Working Party, Guidelines on the Right to Data Portability (2017).

Information Commissioner's Office, *Right of Access* (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

EN

Article 21.

Right to object

Article 21.

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.

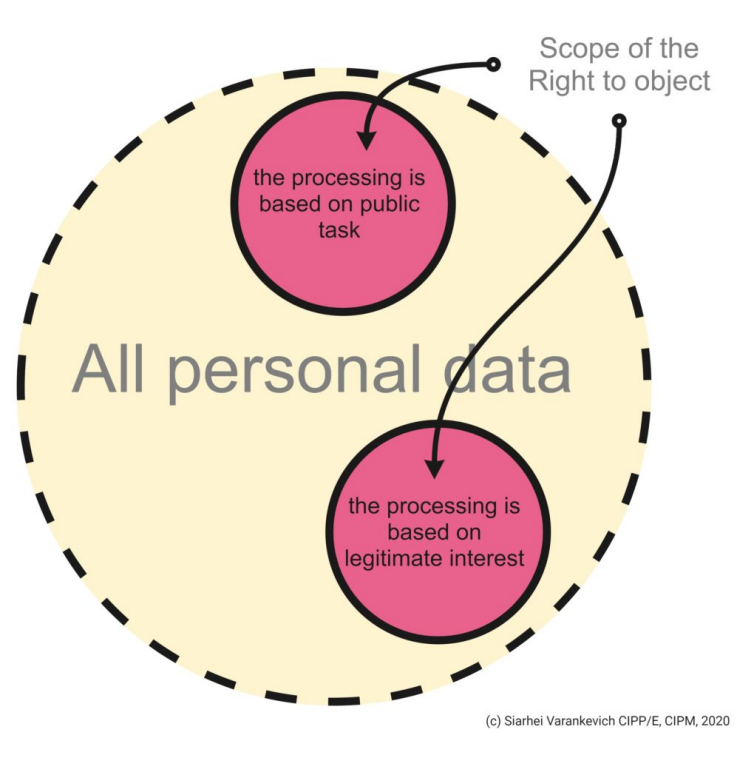
Recitals

(69) Where personal data might lawfully be processed because 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 on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

Expert commentary

Author

Siarhei Varankevich
CIPP/E, CIPM, CIPT, MBA, FIP
Co-Founder & CEO of Data Privacy Office LLC.
Data Protection Trainer and Principal Consultant


Scope of the
Right to object
the processing is based on public task
All personal data
the processing is based on legitimate interest
(c) Siarhei Varankevich CIPP/E, CIPM, 2020

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.

Recitals

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

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, 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.

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 21. Right to object

Expert commentary

Data Subject Request Letter Sample

Concern: Request to stop processing my personal data

Dear Madam, Dear Sir,

You have data concerning me that I am asking you to stop processing.

Pursuant to Article 21(1) of the *General Data Protection Regulation* (GDPR), please stop processing my personal data [*to perform a task carried out in the public interest, according to Article 6(1)(e) of the GDPR*] [*based on a legitimate interest, according to Article 6(1)(f) of the GDPR*].

In consequence, I ask you to delete my personal data and notify every recipient to whom you have disclosed my personal data, pursuant to Articles 17(1)(c) and 19 of the GDPR.

Thank you for confirming as soon as possible that you stop processing my personal data, and in any event within one month of the receipt of my request, according to Article 12(3) of the GDPR.

In the absence of any action taken upon my request in a timely manner, I reserve my right to lodge a complaint with the relevant supervisory authority and seek judicial remedy.

Sincerely,

Data Subject

Author

Louis-Philippe Gratton
PhD, LLM
Privacy Expert

Recitals

(69) Where personal data might lawfully be processed because 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 on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

Guidelines & Case Law

Documents

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).